

In the matter of the General Data Protection Regulation

DPC Case Reference: IN-18-11-1

**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 DPC:

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

Dated 12 December 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

A. INTRODUCTION	1
B. PRELIMINARY MATTERS	3
a) Controller and processor.....	3
b) Competence of the DPC as lead supervisory authority.....	4
C. BACKGROUND	5
a) Overview.....	5
b) Number of EU and EEA users affected by the Breach.....	7
D. CONDUCT OF THE INQUIRY	8
a) Notification and Updates	8
b) Commencement Notice, Queries and Responses	8
c) Correspondence concerning the Expert Measures Review	9
d) Inquiry Report and Response	10
e) Decision-Making Stage	11
f) Fair Procedures.....	11
E. SCOPE OF THE INQUIRY	12
a) Temporal Scope.....	12
b) Material Scope.....	12
F. ISSUES FOR DETERMINATION.....	12
G. ANALYSIS	13
a) Relevant provisions of the GDPR.....	13
b) Analysis of the Issues for Determination	15
i. The Nature, Scope, Context and Purposes of the Processing	17
ii. Analysis of Risk	19
iii. State of the Art	27
iv. Cost of Implementation	29
c) Analysis of the Technical and Organisational Measures Implemented by MPIL	29
i. The Update of the Video Uploader and the Coding of the Access Token.....	30
ii. Design impact of the access token on Logging, Incident Alerting and Detection.....	37
iii. Regular reviews and assessments of the effectiveness of the chosen measures and safeguards	40
(a) Risk reviews.....	40
(b) Security reviews and assessments.....	44
(c) Alternative more appropriate measure	50

(d) Secure coding, policies and training	53
H. FINDINGS	56
a) Finding Regarding Article 25(1)	56
b) Finding Regarding Article 25(2)	57
I. DECISIONS	58
a) Decision on Corrective Powers in Accordance with section 111(2) of the 2018 Act	58
b) Decision Relating to a Reprimand to MPIL Pursuant to Article 58(2)(b) GDPR.....	60
c) Decision Relating to Administrative Fines under Article 58(2)(i) AND 83 GDPR	60
d) ARTICLE 83(2) GDPR	62
i. 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;.....	62
Nature of the Infringements	65
Gravity of the Infringements	66
Duration of the Infringements	67
ii. Article 83(2)(b): the intentional or negligent character of the infringement(s)	67
iii. Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects	71
Incident Response	71
Mitigation of Risks to Third Party Applications	72
Security Enhancements	73
iv. 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	75
v. Article 83(2)(e): any relevant previous infringements by the controller or processor;	75
vi. 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;.....	75
vii. Article 83(2)(g): the categories of personal data affected by the infringement	76
viii. 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;.....	79
ix. 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;	79
x. Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;	79

xi.	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;.....	79
J.	DECISION AS TO WHETHER TO IMPOSE AN ADMINISTRATIVE FINE AND, OF SO, THE AMOUNT OF THE FINE.....	80
K.	ARTICLE 83(3) GDPR	86
L.	ARTICLE 83(4) GDPR	93
M.	Selection of Amounts of Administrative Fines	99
N.	SUMMARY OF CORRECTIVE POWERS.....	105
O.	Appendix: Categories of data affected by the Infringement.....	107

A. INTRODUCTION

1. The General Data Protection Regulation¹ ('**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.
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.
4. On 11 January 2022, the DPC was notified that, effective from 5 January 2022, Facebook Ireland Limited, being the 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 or FB-I, 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 this particular entity is referred to 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), OJ 2016 L 119/1.

6. The DPC commenced an own-volition inquiry under section 110(1) of the 2018 Act (**'the Inquiry'**) on 3 October 2018 in respect of a personal data breach (**'the Breach'**) which was notified to the DPC by MPIL on 28 September 2018.
7. This Decision sets out the findings of the DPC in this matter as to whether (i) one or more infringements of a relevant enactment by MPIL, the controller to which the Inquiry relates, has occurred or is occurring, (ii) if so, whether a corrective power under section 115 of the 2018 Act and Article 58(2) 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.² 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.
8. A preliminary draft version of 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.
9. MPIL made submissions in response to the PDD on 7 February 2023 and, on 27 March 2023, a further response to correspondence from the DPC concerning the PDD.
10. 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.

All submissions made by MPIL in relation to the PDD have been fully considered by the DPC and, 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. As advised in the DPC's letter enclosing the Inquiry Report,³ as this Inquiry concerns matters of cross-border processing, the DPC, as Lead Supervisory Authority, is required to adhere to the One Stop Shop process set out in Article 60 of the GDPR. This requires the DPC to:
 - (i) circulate the Draft Decision to any concerned supervisory authorities for their opinion and

² Sections 105(1) and 107 of the 2018 Act.

³ DPC letter of 12 November 2021. The DPC issued its inquiry report (the **'Inquiry Report'**) to MPIL on 12 November 2021 setting out its views regarding MPIL's compliance in this Inquiry.

- (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.
12. On 24 September 2024 the DPC submitted the Draft Decision to the CSAs for their views, 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.
 13. 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.
 14. No concerned supervisory submitted an objection to the Draft Decision.
 15. 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 fine, pursuant to section 142 of the Act.

B. PRELIMINARY MATTERS

a) Controller and processor

16. 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 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
17. 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

⁴ See, for example, email of 12 October 2018 (containing details on numbers of affected EEA users).

concerned by the 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.

18. 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) Competence of the DPC as lead supervisory authority

19. Chapter VI, Section 2 of the GDPR deals with the competence, tasks and powers of the supervisory authorities.
20. 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.
21. 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 supervisory authority of the 'main establishment' or the 'single establishment' of that controller or processor.
22. 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.
23. 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

⁵ Response First Queries, 2.

⁶ Response First Queries, 2-3.

respect of the personal data pertaining to the Breach, within the meaning of Article 4(23) GDPR.

24. 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

a) Overview

25. The DPC is satisfied, in light of the information provided by MPIL in the Inquiry, that the Breach constituted a personal data breach within the meaning of Article 4(12) GDPR, to which the notification obligation under Article 33(1) GDPR applied. The Breach was notified to the DPC on 28 September 2018 by MPIL. A separate DPC inquiry is examining MPIL's compliance with its notification obligations (the '**Notification Inquiry**').
26. The Breach occurred when an external third party ('**the attacker**') exploited a vulnerability in Meta's codebase ('**the attack**') which allowed the attacker to unlawfully obtain Facebook access tokens⁷ from affected users. Access 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.
27. The vulnerability was caused by the combination of three distinct bugs associated with three distinct Facebook product features interacting with one another, namely 'View As', 'Video Uploader' and 'Happy Birthday Composer'. The vulnerability was introduced into Meta's system in July 2017 upon the modification of the Video Uploader to achieve a new video upload functionality on the Facebook service and remained live until it was remediated after the Breach. The attack occurred between 14 September and 28 September 2018. The attacker accessed Facebook's Video Uploader through the Happy Birthday Composer while in View As mode, and was able to generate fully-permissioned access tokens for other users.
28. MPIL explained how the attack occurred as follows:
- (i) a user's profile was viewed in View As mode triggering the Happy Birthday Composer to render on that user's timeline (for this to happen, that user's birthday was visible on his/her timeline and at least three other users had already posted a 'Happy Birthday' message to that user). MPIL stated:

This was an unknown bug. The View As feature was intended to be purely a 'view only' feature without any 'write' functionality. There was no reason

⁷ Access tokens are described by MPIL in the DPC's Cross-Border Breach Notification Form as 'unique numerical strings that can be used for authentication of a Facebook user account'.

for a user in View As mode to be given the option of sending a Happy Birthday message to themselves.⁸

- (ii) as a result of a modification to the Video Uploader in July 2017 (designed in order to address issues whereby the uploading of a video was disrupted due to a break in internet connectivity), the Video Uploader embedded in the Happy Birthday Composer generated an access token for the View As look up subject, as opposed to the user associated with the profile, who was doing the viewing. MPIL stated:

This was an unintended result of the page generally being rendered as it would be for the View As subject – which caused the access token embedded in the HTML for the video uploader to be generated as it would be for the View As subject. Again, the video uploader – including its corresponding HTML – was not supposed to be part of the page in the first place.⁹

- (iii) the access token, which was a fully permissioned first party token, could then be used to ‘obtain any of the View As subject’s profile information via the Graph API...the token could also be exchanged for a corresponding session cookie, which could then be used to log into the View As subject’s account using a web browser.’¹⁰

29. As a result of the above, MPIL explained, the attacker could move on to target ‘the accounts of users who were friends with any user whose account was controlled by the attacker [the seed users], and to fan out from those accounts to compromise additional users in turn’.¹¹ MPIL outlined that this was achieved on an automated basis using a script.

30. MPIL further explained the attack in its submissions on the Inquiry Report:

[T]he attackers are believed to have deployed an automated script that repeatedly accessed user profiles in View As Specific User mode in order to collect access tokens via the Vulnerability. The script used the access tokens to collect profile data for the affected users through the Facebook Graph API. The script propagated the Attack across a portion of the Facebook social graph (**‘Social Graph’**) by exchanging the stolen tokens for session cookies, which were then used to load more user pages in View As Specific User mode, so that the process could be repeated and the attackers could branch out from one user to the next.¹²

⁸ Response to First Queries, 14.

⁹ Response to First Queries, 14.

¹⁰ Response to First Queries, 14.

¹¹ Response to First Queries, 14.

¹² Submissions on the Inquiry Report, para 6.1.

31. The Breach affected the confidentiality of personal data (i.e. involved a breach of security that led to an unauthorised disclosure of, or access to, personal data).
32. The nature of the personal data affected differed depending on the user account in question. Three different categories of personal data were affected, as communicated by MPIL and are set out in the Appendix to this Decision. These categories included, but were not limited to, personal data such as a user's full name, email address, phone number, location, place of work, date of birth, religion, gender, as well as posts on timelines, group membership, and certain message content. Due to the way in which the attack was carried out, insofar as the attacker had possession of access tokens and session cookies of a large amount of affected users, the attacker had temporary control of a large number of affected user accounts.
33. MPIL submitted that it regarded the severity of the potential impact of the Breach as 'limited' in its update to its breach notification in October 2018 and stated:

[D]ue to the categories of data obtained or exposed and the fact that there was no compromise of high risk elements such as password information, identity documentation, financial information or payment card information, we do not believe that there is a material risk of more extensive harm occurring (such as financial fraud).¹³

34. MPIL was of the view that the main impact of the Breach for affected users would instead be 'an increased likelihood that they will be the target for professional "spam" operations' and that '[t]here may also be an increased risk of individuals being the target for "phishing" attacks'.¹⁴

b) Number of EU and EEA users affected by the Breach

35. The numbers of affected users in the EU and EEA according to the category of personal data affected were provided by MPIL, and are set out below. A total number of 2 983 092 EU and EEA users were affected by the Breach.¹⁵

Location	Category 1	Category 2	Category 3	Total
EU	1 238 390	1 575 747	33 334	2 847 471
EEA	34 207	99 645	1 769	135 621
EU and EEA	1 272 597	1 675 392	35 103	2 983 092

¹³ Updated Cross-Border Breach Notification Form, 17.

¹⁴ Updated Cross-Border Breach Notification Form, 17.

¹⁵ MPIL Submission on PDD, para 3.3. The figure for EU users includes 274 101 users in the UK, which was a Member State of the EU at the time of the Breach.

D. CONDUCT OF THE INQUIRY

The following is a summary of the main stages of the Inquiry to date.

a) Notification and Updates

36. As set out above, MPIL notified the DPC of the Breach on 28 September 2018. MPIL continued to supply information and documentation in relation to the Breach after the notification. Three updates were provided prior to the commencement of the Inquiry between 1 October and 2 October 2018. The fourth update was provided on 12 October 2018 after the Inquiry had commenced.
37. Having reviewed the information provided by MPIL in the breach notification and the first three updates, the DPC formed the view that it was appropriate to assess the subject matter of the Breach in the context of an own-volition inquiry under section 110(1) of the 2018 Act.

b) Commencement Notice, Queries and Responses

38. The Inquiry was commenced by letter dated 3 October 2018 (**'the Commencement Notice'**) under section 110(1) of the 2018 Act. The Commencement Notice set out that the scope of the Inquiry sought to examine whether MPIL had discharged its obligations in connection with the subject matter of the Breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been or was being contravened by MPIL in that context.
39. The DPC raised sixteen queries by letter dated 26 October 2018, addressed to establish the facts as they related to the Breach. MPIL was requested to provide any documentary evidence to support its responses. A response was received together with certain policy documentation (**'Response to First Queries'**) on 23 November 2018. In the course of the Inquiry, the DPC sought and received further responses and submissions from MPIL.
40. On 11 January 2019, MPIL provided the DPC with a post-mortem Incident Report, containing the results of an investigation into the Breach.
41. By letter dated 18 January 2019, the DPC wrote to MPIL attaching an appendix with two further queries arising from information MPIL had submitted in its Response to First Queries. These queries requested information pertaining to the access token involved in the Breach (**'the access token'**).

42. The DPC raised a further twenty-four queries by letter of 7 March 2019 arising from information MPIL had submitted in the Inquiry to that date. The DPC requested that MPIL provide relevant supporting documentation in respect of certain of those queries and sub-queries. MPIL was specifically informed in the appendix to the email that, where relevant supporting documentary evidence was requested in the queries, MPIL was being asked to provide:

original or copies of contemporaneous documentation (including but not limited to notes, communication such as emails, policies and/or procedures and their associated records, incident reports, support tickets etc.) in order to demonstrate how the described activity was conducted.

43. MPIL provided responses in three phases (on 8 April, 18 April and 26 April 2019) in accordance with an agreed timetable (together '**Response to Third Queries**').
44. MPIL provided an update on 14 May 2019 in respect of the re-launch of the View As feature involved in the Breach, and provided a risk assessment in relation to same.
45. By letter of 3 September 2019 the DPC informed MPIL that it had received certain documentation in respect of the Breach from Meta in the context of an associated inquiry (the '**Processor Inquiry**'),¹⁶ which documentation appeared to be relevant to MPIL's obligations under examination in the Inquiry. MPIL was notified that the DPC may rely on those documents which were set out in an appendix to that letter 'as part of its understanding of the facts as they relate to [the Breach]' in respect of this Inquiry.¹⁷
46. By letter of 17 September 2019 the DPC raised three additional queries regarding MPIL's awareness of certain of the said documentation submitted by Meta, as well as whether any steps were taken by MPIL in relation to its obligations as a controller upon becoming aware of the submitted documentation. MPIL responded on 2 October 2019 ('**Response to Fourth Queries**'), and provided an update to its Response to Fourth Queries on 23 March 2020.

c) Correspondence concerning the Expert Measures Review

47. In its Response to Third Queries, MPIL informed the DPC that its external lawyers had engaged an external expert technologist (on a privileged basis) to carry out a review of its technical and organisational measures on its behalf (the '**Expert Measures Review**'). This was in part in response to query 2, which asked whether MPIL had carried out its own Post Mortem/Lessons Learned exercise, and seeking relevant supporting documentary evidence of same between October 2018 and February 2019.

¹⁶ The DPC commenced an inquiry into Meta on 17 October 2018 to examine if Meta had complied with its obligations as a processor in connection with the same Breach at issue in this Inquiry. That Inquiry was discontinued on 10 January 2022 subject to the right of the DPC to utilise submissions from that inquiry in the Inquiry.

¹⁷ DPC letter of 3 September 2019.

48. MPIL gave details of the scope and phases of this Expert Measures Review (without prejudice to its privileged nature) in its Response to Fourth Queries. MPIL provided details of certain improvements implemented or in the course of being implemented on foot of the Expert Measures Review in its update to its Response to Fourth Queries. The Expert Measures Review itself was not provided to the DPC.

d) Inquiry Report and Response

49. By letter of 2 February 2021, the DPC informed MPIL that it was in receipt of information and documentation in respect of the Breach in the context of the associated Processor Inquiry that may be relevant to MPIL's obligations under examination in this Inquiry. MPIL was put on notice by the same letter that the DPC may rely on any of the said information and documentation as part of its understanding of the facts as they relate to the Breach in this Inquiry.¹⁸ MPIL responded by letter of 11 February 2021 reserving its right to make 'submissions in relation to any reliance by the DPC in the Inquiry on information and documentation obtained in the separate inquiry against [Meta] as appropriate in due course'.¹⁹
50. Similarly MPIL was put on notice by letter of 9 February 2021 that the DPC may rely in this Inquiry on any information and documentation received as part of the associated Notification Inquiry which seeks to examine MPIL's notification obligations under Article 33 GDPR. MPIL responded by reserving its right to make submissions. This Decision comprehensively details the information gathered in the Notification Inquiry and the Processor Inquiry that has been relied upon in this Inquiry.
51. The DPC issued its Inquiry Report to MPIL on 12 November 2021 setting out its views regarding MPIL's compliance. MPIL provided its submissions in response to same together with a number of annexures (together the '**submissions on the Inquiry Report**') on 15 January 2022.
52. On 11 February 2022 MPIL provided the DPC with a copy of an expert report carried out by Professor Michael D. Siegel, Director of Cybersecurity at Massachusetts Institute of Technology's Sloan School of Management (the '**Expert Report**'). The letter which enclosed the Expert Report stated that '[t]he Expert Report forms part of [MPIL's] submissions on the Inquiry Report and should be considered alongside and in conjunction with the Response [to the Inquiry Report]'.²⁰
53. The DPC advised MPIL that it would consider the Expert Report (together with the submissions on the Inquiry Report and all other relevant material to the Inquiry) in reaching this Decision notwithstanding that the Expert Report was received after the agreed deadline for receipt of MPIL's submissions on the Inquiry Report.²¹

¹⁸ DPC letter of 2 February 2021.

¹⁹ Letter from Mason, Hayes & Curran ('**MHC**'), solicitors acting on behalf of MPIL, of 11 February 2021.

²⁰ MHC letter of 11 February 2022.

²¹ The deadline for submissions was agreed by the DPC and MPIL as being 14 January 2022.

e) Decision-Making Stage

54. Section 111 of the 2018 Act provides for the decision-making process which applies to this Inquiry, and requires the DPC to consider the information obtained during the Inquiry when deciding whether an infringement is occurring or has occurred and, if so, also provides for a decision on any corrective powers to be exercised. The DPC is required to assess all of the materials and submissions gathered during the Inquiry and any other materials that it considers to be relevant²² in the course of the decision-making process.
55. The DPC notified MPIL of the commencement of the decision-making stage of this Inquiry by letter dated 11 March 2022. For the purpose of enabling the DPC to carry out its decision-making function, the DPC was provided with the Inquiry Report, copies of all documentation annexed to the Inquiry Report (including copies of the breach notification form and any updates thereto), copies of all responses submitted by MPIL in the Inquiry and documentation annexed to same, MPIL's submissions on the Inquiry Report, the Expert Report, as well as copies of all relevant correspondence exchanged between MPIL and the DPC in the Inquiry. The DPC also had copies of all information, documentation, submissions and responses received from MPIL and Meta in the associated Notification and Processor Inquiries respectively.
56. The DPC is satisfied that it has received all relevant materials necessary for it to perform its decision-making function in respect of this Inquiry. In doing so, it is required to carry out an independent assessment of all the materials provided to it by the inquiry team, as well as the submissions made by MPIL on the PDD, and any other information that it considers to be relevant to its decision.

f) Fair Procedures

57. Having reviewed the correspondence in the Inquiry (including representations made by solicitors on behalf of MPIL directed to the fairness of the procedures adopted by the DPC,²³ and a purported legitimate expectation having been articulated by MPIL as having arisen such that a particular procedure would be adopted,²⁴ and considering again the DPC's replies to same²⁵), the DPC is satisfied that the Inquiry was conducted correctly, that MPIL was afforded fair procedures by the DPC throughout the inquiry process and that no legitimate expectation as asserted has arisen. 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 give MPIL the opportunity to provide responses and submissions in respect of the issues under consideration in the Inquiry at appropriate stages, and (iii) to allow MPIL sufficient

²² As already stated, the DPC also considered documentation received from Meta and MPIL in the associated Processor and Notification Inquiries respectively where relevant.

²³ MPIL letter of 7 June 2019.

²⁴ MHC letter of 14 January 2022 and MHC letter of 25 February 2022.

²⁵ DPC letter of 24 June 2019 and DPC letter of 22 February 2022.

time (including extensions of time granted where necessary) to furnish the information and documentation requested by the DPC in the course of the Inquiry.

58. In respect of the articulation of any legitimate expectation, this includes, but is not limited to the position that: (i) the DPC is not bound in law to follow any particular procedure in respect of this Inquiry, (ii) the DPC made no representation, either express or implied to MPIL that any particular procedure in respect of this Inquiry would be followed in this Inquiry up until the DPC's letter of 12 November 2021 (iii) MPIL did not act on faith of any representation or suffer prejudice in reliance on a particular procedure, and (iv) MPIL has had the opportunity to provide submissions on any matter of fact or law in relation to the Inquiry Report, the PDD and the comments of concerned supervisory authorities on the Draft Decision.

E. SCOPE OF THE INQUIRY

a) Temporal Scope

59. The Commencement Notice outlined that the scope of the Inquiry would examine and assess whether or not MPIL had complied with its obligations in connection with the subject matter of the Breach in relation to the processing of the personal data of its users, in order to determine whether or not any provision(s) of the 2018 Act and/or GDPR had been contravened by MPIL in that context.
60. Following intensive examination of the facts in this case, the DPC finds that the material issues in this Inquiry come most properly within the remit of data protection by design and default. Therefore, the questions to be answered in this Decision will cover the implementation of technical and organisational measures pursuant to Article 25 GDPR during the period between 25 May 2018 and the date of the Breach notification on 28 September 2018 (**'the temporal scope'**). For clarity, the findings contained in this Decision do not address, nor are they concerned with, MPIL's compliance with the GDPR in the present day, or prior to the GDPR coming into force on 25 May 2018.

b) Material Scope

61. This Decision considers the application of Article 25(1) and (2) GDPR and the effectiveness and integration of the technical and organisational measures designed and implemented with respect to, inter alia, the access token's design, configuration, purpose, and use by the Video Uploader feature and related features and the fact that such feature were vulnerable to exploitation during the temporal scope.

F. ISSUES FOR DETERMINATION

62. The following issues arise for determination in this Decision:

- (a) An assessment of whether MPIL has complied with its obligations under Article 25(1) and (2) GDPR, which concern the requirements of data protection by design and default.
- (b) This assessment involves consideration of whether MPIL failed to comply with Article 25(1) and/or 25(2) in relation to the effectiveness and integration of the technical and organisational measures implemented during the temporal scope. It includes consideration of the access token's design, configuration, and deployment for use by the Video Uploader.
- (c) This assessment involves consideration of whether the configuration and use of the access token by the Video Uploader for the purpose it was intended,²⁶ was designed to ensure the confidentiality of the personal data, integrated the necessary safeguards in order to meet the requirements of the GDPR and protect the rights of data subjects, and by default only permitted access to such minimum personal data as was necessary for its intended purpose pursuant to Articles 25(1) and 25(2) GDPR.
- (d) This assessment involves consideration of whether MPIL supported its technical and organisational measures with data protection policies which met the principles of data protection by design and default during the temporal scope.
- (e) As Article 25 does not prescribe the implementation of any specific technical and organisational measures or safeguards, the determination of whether data protection by design and default has been achieved must consider whether the measures and safeguards implemented were appropriate having considered the specific processing at issue.

G. ANALYSIS

a) Relevant provisions of the GDPR

- 63. Article 5(1)(c) GDPR provides that personal data shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- 64. Article 5(1)(f) GDPR provides that personal data shall be:
 - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- 65. Article 25 GDPR provides for the protection of personal data by design and default and imposes an obligation on a controller to ensure that it has appropriate technical and

²⁶ MPIL explained to the DPC that purpose of the access token was to enable uploads made through the Video Uploader feature 'to resume exactly at the byte where they left off in the event that a user's internet connection was disrupted during upload' (First Queries, 14).

organisational measures in place designed to implement the data protection principles as outlined in Article 5 GDPR.

66. Article 25(1) GDPR provides for Data Protection by Design:

Taking into account the state of the art, the cost of implementation and the nature, scope and context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

67. Article 25(2) GDPR provides for Data Protection by Default:

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

68. Recital 78 GDPR is closely associated with Article 25 GDPR, and provides assistance in its interpretation. Recital 78 provides:

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met.

In order to be able to demonstrate compliance with this Regulation, the controller should **adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.** [Emphasis added.]

Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. [Emphasis added.]

The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

b) Analysis of the Issues for Determination

69. The assessment of MPIL's compliance with Article 25(1) and (2) must have regard to the nature, scope, context and purposes of this processing and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the relevant processing. In assessing MPIL's compliance with Article 25(1) and (2), The DPC must also take into account the state of the art and the cost of implementation.
70. Article 25(1) obliges a controller to implement appropriate measures to implement the GDPR data protection principles of Article 5(1) in an effective manner in any processing system both at the design phase and at the time of processing itself.
71. Article 25(2) obliges a controller to implement appropriate measures to ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed, and that by default personal data are not made accessible without the data subject's intervention to an indefinite number of natural persons.
72. MPIL should be able to demonstrate that it has implemented internal policies which meet in particular the principles of data protection by design and default required by Article 25.
73. The European Data Protection Board ('EDPB') has published Guidelines on Data Protection by Design and by Default, which summarises Article 25 as follows:

The core of the provision is to ensure appropriate and effective data protection both by design and by default, which means that controllers should be able to demonstrate that they have the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.²⁷

²⁷ EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and Default*, (Version 2.0, Adopted on 20 October 2020), 5 ('Article 25 Guidelines').

74. The EDPB explains the concept of ‘appropriate’ technical and organisational measures, and its close connection with effectiveness as follows:

Technical and organisational measures and necessary safeguards can be understood in a broad sense as any method or means that a controller may employ in the processing. Being appropriate means that the measures and necessary safeguards must be suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness.²⁸

75. For clarity, in determining, designing and implementing measures, the DPC acknowledges that a standard of perfection is not the standard required by the GDPR under either Article 25(1) or (2).²⁹ Rather, under Article 25(1) controllers are required to implement appropriate technical and organisational measures that ensure that all of the data-protection principles, set out in Article 5 GDPR, are implemented in an effective manner which integrates the necessary safeguards into the processing. In this context, MPIL is required to plan, implement and demonstrate appropriate technical and organisational measures and safeguards in every layer of its processing, including at the point of the design of its processing systems and technologies. These activities must be done to effectively minimise the risk to the data-protection principles regarding the personal data that MPIL processes, as well as to minimise the risks to the ongoing resilience of its processing systems.
76. This standard of appropriateness also applies to measures required to be implemented under Article 25(2).
77. MPIL’s existing technical and organisational measures in place at the time GDPR took effect on 25 May 2018 must comply with Article 25 from that date and throughout the temporal scope of the Inquiry. The EDPB has confirmed that legacy systems designed pre-GDPR became subject to Article 25 obligations:

The requirement described in Article 25 is for controllers to have data protection designed into the processing of personal data and as a default setting and this applies throughout the processing lifecycle. [Data protection by design and default] is also a requirement for processing systems pre-existing before the GDPR entered into force. Controllers must have the processing consistently updated in line with the GDPR.³⁰

²⁸ Article 25 Guidelines, 6.

²⁹ As argued by MPIL in its Submissions on the Inquiry Report, paras 11.2 and 11.6 (e).

³⁰ Article 25 Guidelines 5.

78. The DPC considers that the central matters for determination are whether MPIL implemented appropriate technical and organisational measures pursuant to its obligations under Articles 25(1) and 25(2) respectively. In assessing whether MPIL complied with its obligations in this regard, the DPC must have regard to the state of the art, the cost of implementation and 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 posed by the processing during the temporal scope. For the purpose of its analysis in this Decision, the DPC has avoided applying hindsight based on what subsequently became known after the Breach, and the content of lessons learned exercises undertaken by Meta and MPIL and provided to the DPC in the context of this Inquiry to improve their measures.

i. The Nature, Scope, Context and Purposes of the Processing

79. As set out above, access tokens are provided to users following successful authentication of their login details, and allow the user to perform certain actions relating to that Facebook user account. These tokens enable access to users' Facebook Accounts. Therefore, in respect of its consideration of the nature, scope, context and purposes of the processing, the relevant processing of personal data to which the DPC must have regard concerns the processing that MPIL undertook in respect of each Facebook user's account. This processing includes personal data shared or otherwise communicated in the context of social media activities.

80. The nature of processing refers to the basic or inherent features of the operations performed on personal data by a controller. Facebook is a social media service available at the website www.facebook.com, and as an app for Android and iOS. Users with a Facebook account can create a profile containing personal information, photos and interests, and connect with other users by adding them as 'Friends', or (usually in the case of people they do not know personally) by 'following' another user's profile. Each user's profile includes their 'Timeline', where they can post photos, videos, locations and status updates, as well as see posts they have been 'tagged' in and posts written to their Timeline by Friends. Users can also create and manage 'Pages,' 'Groups' and 'Events' around particular interests, topics or social activities. The homepage that a user sees when they log into their account contains a 'Newsfeed' showing a list of status updates, photos, videos and 'likes' by other users, Pages and Groups that they follow on Facebook, which is continuously updated. Users can 'like' or comment on other users' posts, 'tag' other users in posts, send messages to other users, and create a 'Facebook Story' which remains visible for 24 hours, among other features. The audience of content that users share on Facebook can be edited depending on who the user wishes to see it (alternatives include 'Public', 'Friends' or 'Custom.') There is an option to remove (or 'Unfriend') a person whom the user had previously added as a Friend, and users can 'block' other users to prevent them from (for example) seeing their profile or sending

them messages. The DPC considers that the nature of the processing is expansive and complex.

81. The scope of processing refers to the extent of operations performed on personal data by MPIL. The processing carried out for the purpose of providing the Facebook service involves a wide range of types and categories of personal data (including children's data) in high volumes. This is reflected in the record of processing provided by MPIL for the purpose of Article 30 GDPR in the Inquiry,³¹ in the range of features of the Facebook service that users interact with regularly, and in the number of users of the Facebook service within the EU/EEA for whom MPIL has confirmed it is responsible as the controller. Facebook is a popular and widely used social media service. Facebook had 2.32 billion³² monthly active users globally as of 31 December 2018.³³ Further, the DPC understands that in Q4 2018, when this Inquiry was commenced, Facebook had 381 million monthly active users in the EU. The personal data typically processed includes special category data. For example, MPIL confirmed that data revealing religious beliefs (a special category of data pursuant to Article 9(1) GDPR) were affected by the Breach. MPIL also confirmed that data revealing gender and relationship status were affected and that an affected user, when selecting 'relationship status', could indicate on their Facebook profile whether the user is single, married or divorced. The DPC considers that details on marital status constitute special category data in terms of being 'data concerning a natural person's sex life' and rejects MPIL's submission that a person's relationship status cannot by itself constitute special category data, particularly when other exposed information can make it easy to identify other persons involved in such relationships, such as cohabitants or romantic partners.³⁴ Therefore, the DPC also considers that special category data, in the form of 'data concerning a natural person's sex life or sexual orientation' as defined by Article 9(1) GDPR, were affected by the Breach.
82. The context of processing refers to the circumstances that form the setting of the processing. MPIL submits that the Facebook service is unique in its nature, scope, complexity and scale of its processing, and that it runs on a large and complex codebase encompassing multiple millions of lines of code which is constantly evolving.

³² In this Decision, the DPC is using the short numeric scale definition of the word 'billion' to mean 10⁹. 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.

³³ Press Release, 'Facebook Reports Fourth Quarter and Full Year 2018 Results' (30 January 2019), available at: <https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx>.

³⁴ See in this regard the observations of the CJEU in Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601, paras 122-127.

83. The purposes of processing refers to the reasons for processing personal data. The purposes of the processing in respect of each Facebook user's account relates to the provision of the Facebook service, as outlined above, to Facebook users. The purpose of the access tokens is to allow Facebook users to perform certain actions relating to their Facebook user account. These purposes seek to enable users to view and inspect their own personal Facebook page from the perspective of another user via the View As feature. Therefore, the purposes of the processing are closely related to the provision, personalisation and improvement (in the sense of the improvement of the user experience) of the Facebook product; which purpose is explicitly specified in the Record of Processing provided by MPIL during the Inquiry.³⁵
84. The DPC does not accept the view expressed by MPIL in its submissions on the PDD that:
- [t]he nature, scope, and purpose of the relevant processing operation are the nature, scope, and purpose of the uploading of videos that the Video Uploader Token was designed to support – all of which were far more limited than the nature, scope, and purpose of the operation of the entire Facebook service.³⁶
85. While the intended purpose of the use of access tokens that contributed to the Breach was, as MPIL submits, limited to uploading of videos, those tokens could be used to give access to the full contents of users' accounts. However unintended, that degree of access necessarily brings into the scope of processing the wider range of processing carried out through Facebook user's accounts. The extent of access to personal data provided by the tokens used went beyond the intended purpose of processing for this feature.
86. In light of the matters outlined above, the DPC agrees with the inquiry team's view expressed in the Inquiry Report, that the nature, scope, context and purposes of MPIL's and Meta's processing indicated that it was 'expansive in nature, broadly-scoped, contextually extensive, and undertaken for wide-ranging purposes.'³⁷

ii. Analysis of Risk

87. In implementing measures pursuant to Article 25(1) and (2) GDPR, MPIL must have regard to the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the relevant processing.

³⁵ MPIL Record of Processing, 1.

³⁶ MPIL Submissions on the PDD, para 4.5.

³⁷ Inquiry Report, para 154.

88. Recital 76 GDPR provides guidance as to how risk should be evaluated:

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

89. Recital 75 GDPR enumerates further examples of risks to the rights and freedoms of natural persons from processing of personal data, of varying likelihood and severity, which could lead to physical, material or non-material damage. It particularises the processing of children's personal data, personal data revealing religion, personal data concerning sex life, and processing which involves a large amount of personal data and affects a large number of data subjects, all of which the DPC considers to have been involved in the processing subject to the Breach.

90. Specifically regarding the risk of personal data breaches, types of physical, material or non-material damage which can result to data subjects are outlined in Recital 85 GDPR, which states:

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

91. The European Data Protection Board has stated:

29. The GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing).

30. When performing the risk analysis for compliance with Articles [sic] 25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments...

32. ...controllers ...must always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed...³⁸

92. Therefore, in complying with the requirements of Article 25(1) and (2), in the first instance, it is appropriate to identify the risks to the rights of data subjects that a violation of the principles presents. One must have regard to the likelihood and severity of those risks and must implement measures to effectively mitigate them.
93. It is clear that MPIL's processing of users' personal data, including its use of access tokens, presented risks relevant to a number of the data protection principles provided for in Article 5 GDPR. In assessing MPIL's compliance with Article 25, the DPC must have regard to the risk of bad actors using compromised access tokens to gain access to the personal data of Facebook users. This risk, for example, relates to the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR. This principle requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.
94. The DPC considers that the likelihood of the risks posed by MPIL's processing of personal data was moderate to high. Specifically, it considers that there was a moderate to high risk of the exploitation of a software flaw in the codebase, resulting in personal data breaches. During the Inquiry, MPIL submitted that it can only 'take into account risks that it can reasonably foresee'³⁹ and that the 'appropriateness' of its measures must be assessed based on the risks that were reasonably foreseeable to it at the relevant time.
95. MPIL made various submissions that the specific risk or likelihood of the vulnerability and the Breach occurring as it did was not reasonably foreseeable or 'known' to MPIL or Meta, and that it involved an 'obscure interaction of multiple features on the Facebook website that were neither intended nor anticipated to be used together in practice'.⁴⁰
96. MPIL submitted:
- This was an unprecedented attack on Facebook, there had never been any incident in which millions of accounts were suddenly compromised and there was no known vulnerability that could allow such an event to occur.⁴¹
97. The DPC has also considered the opinion of Professor Michael Siegel in the Expert Report, who argued in support of MPIL that the vulnerability and/or the attack were not foreseeable. Professor Siegel stated:

³⁸ EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and Default*, (Version 2.0, Adopted on 20 October 2020), 5 ('Article 25 Guidelines') 9.

³⁹ Submissions on the Inquiry Report para 13.2.

⁴⁰ Submissions on the Inquiry Report para 13.5.

⁴¹ Submissions on the Inquiry Report para 16.24. MPIL made a similar argument in its Submissions on the PDD, 11-14.

The Vulnerability involved the unexpected interaction of three distinct and unrelated features, under a specific and uncommon set of conditions that created a novel mechanism by which an attacker could generate access tokens for other users. There was no reason for [MPIL] or its processor [Meta] to be specifically aware of this code interaction prior to the Attack, let alone the Vulnerability, given that this code interaction did not involve an intended use case for the features in question and arose only in unusual, isolated circumstances.⁴²

98. The DPC considers that, while that attack may have been unprecedented, the nature of the attack (the exploitation of a software flaw in a highly complex codebase introduced by a change of code), and the concomitant risk to Facebook users, was not. Chris Morales, cybersecurity expert and Head of Security Analytics at Vectra, in a statement relied upon by MPIL in its submissions on the Inquiry Report (in support of its remediation efforts), recognised in respect of the vulnerability that led to the Breach that:

[t]his type of compromise of a software flaw isn't surprising. All code has these forms of flaw that allow unintended use of software and the more complex the software gets the more likely these type of flaws exist.⁴³

99. The analysis of risk relevant to this Decision does not relate to the likelihood of any single specific personal data breach occurring. The DPC considers that the GDPR does not require a controller to foresee or have experience of a **particular breach** or **particular vulnerability** in order to design and implement appropriate technical and organisational measures. The purpose of data protection by design and default is to be prospective and preventative, and not to impose a limited retroactive standard such that controllers are obliged to implement measures only in respect of a vulnerability that has already occurred, or of which the controller has prior experience. This would defeat the purpose of data protection by design and default, which is to identify and reduce (and prevent where possible) granular risk in the architecture supporting the processing, before those risks may combine to give rise to a breach, novel or otherwise.
100. As already noted, MPIL stated that the code responsible for generating the exploited access token 'consisted only of several lines of code, in a codebase for the Service encompassing tens of millions of lines of code'. The DPC agrees with the inquiry team when they recognise that there is an 'inherent risk of software bugs and vulnerabilities in maintaining such a large and complex codebase'.⁴⁴ The DPC considers that there is an inherent and heightened risk in such a vast and complex codebase involving multiple features. Given the interplay between so many features in such a large service, it could

⁴² Expert Report, 1.

⁴³ Submissions on the Inquiry Report, para 17.6(a). MPIL describe Vectra as a private enterprise that specialises in AI threat detection and response.

⁴⁴ Inquiry Report, para 151.

be expected that modifications in one feature could inadvertently but negatively impact the functionality of another feature, such as was seen in the case of the Breach. Separately, it must be noted that the authorisation mechanisms used by the Facebook service are of utmost importance to protect the accounts and personal data of the users to whom the authorisation controls apply. Given the heightened inherent risks associated with such a large codebase consisting of various features and functionalities which interact in complex ways, the measures and safeguards put in place to authorise control over user accounts should be appropriate to the risks. The overarching importance of reducing risk and applying appropriate measures and safeguards in every layer of the processing is therefore evermore apparent.

101. The DPC considers that the severity of the risk for rights and freedoms of natural persons posed by the processing was moderate to high. As illustrated by the personal data breach, this processing includes the risk of bad actors gaining access to personal data such as a Facebook User's full name, email address, phone number, location, religion, gender, relationship status, as well as posts on timelines, group membership, and certain message content. This access poses particular threats to data subjects regarding being targeted for spam operations and phishing attacks (which MPIL indicate are the most likely impacts of the Breach). In the course of the inquiry, MPIL stated, in response to the DPC's query '[h]ow severe are the potential impacts for affected individuals?' that it believes:

the main impact for affected users will be an increased likelihood that they will be the target for professional 'spam' operations. There may also be an increased risk of individuals being the target for 'phishing' attacks.⁴⁵

102. The DPC does not agree with MPIL's argument in its Submissions on the PDD that the severity of the risk posed by the processing should be assessed by reference only to the uploading of videos using the Video Uploader Token.⁴⁶ As discussed at paragraphs 83-86 and elsewhere in this Decision, the foreseeable consequences of using those tokens in the way that MPIL did brought into scope a range of personal data and processing that greatly exceeded the uploading of videos.
103. The DPC considers that phishing attacks (particularly where multiple data points were exposed concerning data subjects at large scale), carry significant risk and, as MPIL recognises, spam 'can be used as a vector for phishing messages'.⁴⁷ The DPC considers

⁴⁵ Updated Cross-Border Breach Notification Form, 17, in which MPIL provided an update to section 5.6, which sought information about the severity of the potential impacts of the Breach for affected individuals. The DPC notes MPIL later asserted that there [REDACTED]

[REDACTED] and contended that the most likely risk to affected users is through spamming operations such as mass-marketing and advertising. See Submissions on the Inquiry Report, para 19.8.

⁴⁶ MPIL Submissions on the PDD, 7 February 2023, para 5.13-15.

⁴⁷ Submissions on the Inquiry Report, para 19.9.

that phishing scams are a means to defraud users to obtain sensitive information such as personal identity details, bank account details, credit card numbers, and passwords potentially resulting in major financial loss and distress to the user. (The DPC acknowledges however that MPIL has stated that financial data were not directly impacted by the Breach). Additionally phishing emails may harbour viruses and other harmful programs, and may download malware which can lock the user out of vital programs, provide unauthorised access to sensitive information, or crash the user's entire system. The European Union Agency for Cybersecurity ('ENISA') states:

[Phishing attacks] involve a combination of social engineering and deception. The attack usually takes the form of SPAM mail, malicious Web sites, email messages, or instant messages, appearing to be from a legitimate source such as a bank, or a social network. The attackers often use scare tactics or urgent requests to entice recipients to respond, and these fraudulent messages **are usually not personalized** and may share similar generic properties.⁴⁸[Emphasis added]

104. The wide-ranging nature of the personal data that can be exfiltrated from Facebook Accounts increases the risk that more targeted 'spear phishing' attacks may be carried out on users, where the attackers impersonate a trusted source, using the personal data obtained in a personal data breach, making the attack more personal and more likely to be successful. ENISA describe spear phishing as the following:

Spear phishing is a more sophisticated and elaborate version of phishing. It targets specific organisations or individuals, and seeks unauthorized access to confidential data. Just like in standard phishing, spear phishing attacks impersonate trusted sources. Moreover the attacks are personalised, and tactics such as sender impersonation are used.

Attackers may use public information found on social media sites such as LinkedIn or Facebook and personalize their message or impersonate users so that the spear phishing email is likely enough, and the targeted users feel compelled to react to it.⁴⁹

⁴⁸ ENISA 'Phishing/Spear phishing' available at:
<https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing>.
(Retrieved 16 April 2024.)

⁴⁹ ENISA 'Phishing/Spear phishing'.

105. MPIL infers in its submissions on the Inquiry Report that the responsibility rests with the victim of a phishing attack to avoid adverse effects and ensure they are not defrauded, notwithstanding that the attacker was given the means to target the user by MPIL. MPIL submitted:

[MPIL] does not dismiss the problem of spam, particularly to the extent that it can be used as a vector for phishing messages. That is why, when affected users were informed about the Breach, the communications to users provided a link to guidance on the Facebook Help Centre explaining steps that users could take to help protect themselves from suspicious emails or text messages. **However spam and phishing messages have long been ubiquitous for email or mobile users. Any increase in the risk of such communication being sent to users affected by the Attack was likely to be marginal. Moreover, such messages are often blocked by spam filters, and those that are not can easily be deleted or ignored by users.**⁵⁰[Emphasis added]

106. The DPC considers the preceding statement flawed and that it attempts to normalise and trivialise the occurrence of spam and phishing attacks, minimise their potential severity, consequences for the user and inherent criminal nature, and does not accord with the GDPR's emphasis on the primacy of the protection of the rights and freedoms of natural persons, the respect for private life, and the protection of personal data as a fundamental right as guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights.
107. In addition to the risk of spam and phishing attacks, the DPC considers that the types of personal data processed by MPIL also increases the severity of the risk. The DPC notes that the types of data affected by the Breach included personal data likely to carry a high risk as considered by the Article 29 Working Party of the EU data protection authorities (WP29), who published guidelines⁵¹ which have been endorsed by the EDPB. The guidelines list certain criteria which may indicate high-risk processing, the processing of two or more of which require a Data Protection Impact Assessment pursuant to Article 35 GDPR. These indicators of high-risk processing include special category data, children's personal data and large-scale processing, all of which were affected by the Breach, notwithstanding MPIL's assertion that the attack 'did not target minors' data nor did it significantly implicate [special category data]'.⁵²

⁵⁰ Submissions on the Inquiry Report, para 19.9. The DPC notes that MPIL maintains that it informed EU users on a voluntary basis and not because the Breach was likely to result in a high risk to their rights and freedoms pursuant to Article 34 GDPR.

⁵¹ WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in high risk' for the purposes of Regulation 2016/679, adopted 4 April 2017, revised and adopted 4 October 2017.

⁵² Submissions on the Inquiry Report, para 19.3.

108. As discussed above, the DPC considers three categories of special category data carrying significant risks for the rights and freedoms of affected users by reason of their nature as being particularly sensitive were affected by the Breach. The DPC notes that special category data merits enhanced protection under GDPR, and Recital 52 GDPR recognises that their processing could create significant risks to the fundamental rights and freedoms of data subjects. The DPC has also taken into consideration that the CJEU has recognised that the processing of special category data is liable to present ‘a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter [of Fundamental Rights of the European Union]...’.⁵³
109. Certain of MPIL’s submissions on the Inquiry Report address the issue of whether the Breach caused actual material or other effects,⁵⁴ or resulted in actual harm to EEA/EU users. The DPC notes MPIL maintains that it is ‘unaware of any harm’⁵⁵ that resulted from the Breach, believes any risk of harm ‘was always low’,⁵⁶ and that MPIL considers the severity of the potential impact of the Breach to be ‘limited’.⁵⁷ MPIL argues in its submissions on the Inquiry Report:
- [T]here is a clear distinction between ‘risks’ arising from the Breach and ‘effects’ occurring as a result of the Breach. More than three years on from the Attack, [MPIL] is not aware of any adverse effects, material or otherwise, that have been suffered by the data subjects involved in the Attack as a result of their data being accessed as part of the Attack. The Inquiry Report does not specify any such effects, nor does it cite any evidence of such effects occurring.⁵⁸
110. It is not the purpose, nor would it be possible, for this Inquiry to investigate and establish how these risks may have materialised for individual EU/EEA users. The DPC rejects any proposition that it is required to prove specific harm in order to make a finding that the processing posed a high risk to rights and freedoms of affected users.⁵⁹ Rather, in terms of assessing whether MPIL complied with its obligations under Article 25(1) and (2) of the GDPR, it is necessary to assess the level of risk posed by MPIL’s processing during the temporal scope. While the personal data breach that occurred reflects the

⁵³ Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601, para 126.

⁵⁴ For example, MPIL states that the ‘Inquiry Team provides no explanation for its finding that the Breach caused material or other effects other than citing the occurrence of the Breach itself... [t]he ‘unauthorised disclosure of, or access to, personal data’ cannot be considered a harm separate from the data breach itself – that is part of the very definition of a personal data breach under Article 4(12) GDPR.’ See Submissions on the Inquiry Report, para 19.4.

⁵⁵ Submissions on the Inquiry Report, para 19.1.

⁵⁶ Submissions on the Inquiry Report, para 19.1.

⁵⁷ Updated Cross-Border Breach Notification Form, 17.

⁵⁸ Submissions on the Inquiry Report, para 19.5.

⁵⁹ As can be inferred by MPIL’s statement ‘[a]bsent a specific risk of data being used to cause some identifiable harm, the mere fact that the data has been accessed by unauthorised actors does not by itself provide a basis to conclude that users face a high degree of risk’. MPIL Submissions on the Inquiry Report, para 19.6 (c)(iii).

realisation of some of those risks, it is not determinative of the level of risk relevant to the assessment under Article 25(1) and (2). Rather, this assessment must focus on the potential risks that MPIL ought to have been aware of during the temporal scope. The DPC considers that MPIL ought to have been aware of certain risks associated with the processing at the time of the Breach, which were components in the root cause of the Breach (notwithstanding that MPIL carried out no risk assessment into the new usage of the access token by the Video Uploader during the temporal scope to support its assertion that the risk was unforeseeable). Prior to the Breach, MPIL and/or Meta were aware the access token was overly permissioned,⁶⁰ that the access token should not have been used by the Video Uploader beyond testing, and that it presented an attack surface which could be exploited if the token were to be exposed to unauthorised parties. The DPC considers that MPIL **ought to have been** aware of inherent risks associated with processing which relies upon the generation of an access token (which serves an authentication/authorisation function), and **ought to have been** aware that wherever there is **any** token generated by a piece of code there is a risk that it will be misused by unauthorised parties, or that it could potentially be generated in unanticipated contexts. These security risks, together with MPIL's awareness or otherwise of same, are considered more fully later in this Decision.

111. In light of the above and for the purpose of its analysis in this Decision, in consideration of the nature, scope, context and purposes, the DPC considers that the processing that MPIL undertook in respect of each Facebook user's account objectively presented a risk of moderate to high severity, and of moderate to high likelihood, to the rights and freedoms of its users during the temporal scope, in respect of which MPIL was obliged to limit that risk by implementing and appropriate technical and organisational measures.

iii. State of the Art

112. The controller must take account of 'state of the art' when determining the technical and organisational measures applicable to its processing. The Article 25 Guidelines provide guidance on the interpretation of 'state of the art' as referred to in the GDPR.

⁶⁰ MPIL advised the DPC that Meta's security team identified certain risks with the access token in December 2017, which were unresolved during the material scope (and at least one of which was a factor in the Breach). MPIL submitted that it was aware in December 2017 of the risk that the access token carried 'full API permissions, meaning that a token with this app ID provides full access to the data in a user's account', see MPIL Response 14 March 2019 (Processor Inquiry), 5. MPIL acknowledge that the fully permissioned access token was a factor in the Breach, stating 'in particular, the Post Mortem Report specifically described the fully permissioned nature of the Video Uploader token and explained how it was one component of the root cause of the attack'. Submissions on the Inquiry Report, para 17.12.

113. The controller is under an obligation:

to take account of the current progress in technology that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances;⁶¹

...

The 'state of the art' is a dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed *continuously* in the context of technological progress.⁶²

114. In this regard, the DPC notes and endorses the reliance placed by the Inquiry Team in its work on relevant expert guidance from ENISA, the US National Institute for Standards and Technology, the International Organization for Standardisation and the Open Web Application Security Project.⁶³

115. In its submissions on the PDD, MPIL referred to a Decision of the DPC dated 15 March 2021 in which the DPC had examined MPIL's technical and organisational measures including those dealing with software vulnerability and bug management.⁶⁴ MPIL pointed out that, in that Decision, the DPC had found that the information provided during that Inquiry did not show that a failure by MPIL to have in place technical and organisational security measures appropriate to the risk associated with the processing, and that the information provided by MPIL indicated:

...an approach to security at [MPIL] and [Meta] that, in many respects, could be considered analogous to industry best practice and the state of the art, in terms of the breadth of areas relevant to security it covers.⁶⁵

116. MPIL submitted that 'the product security controls at issue [in the present case] are the same controls as were at issue in [the other Inquiry referred to], and there is no apparent reason to regard them as less reflective of industry best practice or state of the art now.'⁶⁶

117. The DPC does not agree with that submission. As MPIL noted,⁶⁷ the DPC's conclusions on the other Inquiry referred to were 'strictly without prejudice to any other ongoing assessment of MPIL's compliance with Articles 5(1)(f) and 32 in respect of the relevant period.' Moreover, that Decision and the findings made in it were based on the

⁶¹ Article 25 Guidelines, para 19. Emphasis in original.

⁶² Article 25 Guidelines, para 20. Emphasis in original.

⁶³ Inquiry Report, para C.3.

⁶⁴ MPIL Submissions on PDD, para 6.4-6.

⁶⁵ Decision of the DPC concerning MPIL in Inquiry IN-18-11-5, 15 March 2021, para 130.

⁶⁶ MPIL Submissions on PDD, para 6.5.

⁶⁷ *ibid.*

documentary and other evidence provided to the relevant Inquiry, and were addressed only to the facts in issue in that case. That Decision did not consider the attack, the Breach or the vulnerability that allowed them to happen. The DPC therefore does not accept that its views expressed in a Decision on separate issues should determine its assessment in this case.

iv. Cost of Implementation

118. The cost of implementation is a factor to be taken into account when selecting appropriate technical and organisational measures. In particular, the Article 25 Guidelines indicate that the cost (including financial, time and human resources) should not be disproportionate, in the sense that the controller may opt for an alternative, less costly measure where it is demonstrated to be equally as effective at achieving a level of security appropriate to the risk.⁶⁸ In light of the scale of financial turnover of MPIL and Meta this element is likely to have a minimal weighting.
119. In its submissions on the PDD, MPIL observes that the risk-based approach to security provided for in Article 25 GDPR requires controllers to allocate human and financial resources according to the risk posed by the processing, and that this is the premise of the 'cost' factor provided for in Article 25(1).⁶⁹ The DPC agrees that the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing forms one aspect of the decision to implement appropriate measures. However, Article 25 requires other matters to be taken into account, including the nature, scope, context and purposes of processing.
120. The DPC does not accept that the approach adopted by MPIL in the present case was compliant with its Article 25(1) GDPR obligations. The risks posed by the over-permissioned Video Uploader access token and the other vulnerabilities that contributed to the Breach were, particularly in the context of the quantity and types of personal data processed on or through the Facebook platform, clearly foreseeable – and in some cases were in fact foreseen – by MPIL. In view of the human and technical resources available to MPIL, a more secure resolution of those risks could and should have been achievable with relatively little cost in both financial and human resources. The DPC therefore rejects MPIL's assertion that 'the DPC has no basis to discount or minimise the relevance of the "cost of implementation" as a factor in its analysis.'⁷⁰

c) Analysis of the Technical and Organisational Measures Implemented by MPIL

121. MPIL has set out its technical and organisational measures concerning the processing subject to the Breach during the temporal scope in its various submissions. In assessing MPIL's compliance with Article 25(1) and (2) GDPR all such submissions, exhibits and documentation have been considered in full.

⁶⁸ Article 25 Guidelines, 8-9.

⁶⁹ MPIL Submissions on PDD, 7 September 2023, para 7.2.

⁷⁰ *ibid*, para 7.3.

122. The DPC has not considered materials related to the Expert Review, or changes or improvements MPIL made to its measures following the commencement of the Inquiry (which are not relevant to the issue of MPIL's infringement of or compliance with the GDPR during the temporal scope). Those measures which relate to changes or improvements which MPIL has made in the intervening period will be addressed, insofar as relevant, in the section of this Decision setting out the DPC's decision on corrective powers in accordance with section 111(2) of the 2018 Act below.

i. The Update of the Video Uploader and the Coding of the Access Token

123. MPIL submitted that the vulnerability exploited by the attacker was introduced into the Facebook service on 12 July 2017, when the code for the existing Video Uploader feature web platform was modified so as to achieve a new processing operation through the generation of a particular type of access token. The purpose of the modification and the access token was to permit the user to resume video uploads in the event of disruption or disconnection. The initial design of the new processing operation (e.g. the modification of the Video Uploader to generate an access token, the coding and permissions of the access token itself at the point of design, and its use to obtain a session cookie that permitted full access to a targeted user's account), in July 2017 falls outside the temporal scope of this Inquiry, as it predates the GDPR coming into force on 25 May 2018.

124. Article 25(1) of the GDPR establishes that a controller has a core obligation to effectively implement the data protection principles of Article 5 of the GDPR by design, and requires that data protection by design must be implemented in the selection of appropriate technical and organisational measures both at the time of determining the means of processing and continually 'at the time of the processing itself'.⁷¹

125. While, the initial design of the software that modified the Video Uploader and the coding of the access token is not in scope of this Inquiry, its continued use, design and default configuration as it applied to the processing during the temporal scope falls to be considered by the DPC in assessing MPIL's compliance with GDPR. In respect of this period, in order to ensure effective data protection at the time of processing, MPIL was required to 'regularly [review] the effectiveness of [its] chosen methods and safeguards.'⁷²

126. The EDPB states:

Once the processing has started the controller has a continued obligation to maintain [data protection by design and default], i.e. the continued effective implementation of the principles in order to protect the rights, staying up to date on state of the art, reassessing the level of risk, etc. The nature, scope and context

⁷¹ Emphasis added.

⁷² Article 25 Guidelines, 4.

of processing operations, as well as the risk may change over the course of processing, which means that the controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen methods and safeguards.

The obligation to maintain, review and update, as necessary, the processing operation also applies to the pre-existing systems. This means that legacy systems designed before the GDPR entered into force are required to undergo reviews and maintenance to ensure the implementation of measures and safeguards that implement the principles and rights of data subjects in an effective manner, as outlined in these Guidelines.⁷³

127. MPIL explained in the associated Processor Inquiry that the [REDACTED]

[REDACTED] MPIL stated:

At the time, Facebook already had a functioning byte-level resumable video upload service that was compatible with Facebook first-party mobile apps, including Facebook for Android (the 'Upload Service'). [REDACTED]

[REDACTED]⁷⁴

128. After a number of documented failed attempts, the developer responsible for specifying the app ID for the access token configured the access token to use the Facebook for Android app ID ('FB4A app ID'), which was designed specifically for the requirements of mobile use and not web-based use, and did not reflect the type of application for which the token was being generated (as MPIL stated was the purpose of specifying the app ID).

129. MPIL submitted:

The code that generated the Video Uploader Token did so by calling to an internal Facebook API, which would return an access token for the user (which in turn would be embedded in the page HTML). [REDACTED]

[REDACTED] The 'app ID' that the

⁷³ Article 25 Guidelines, 10- 11. Emphasis added.

⁷⁴ MPIL Response 14 March 2019 (Processor Inquiry), 4.

developer selected for this parameter was the app ID for the Facebook for Android app (the 'FB4A app ID').⁷⁵

130. This technical measure was selected, not because it was the most appropriate measure to achieve its intended purpose and safeguard the rights and freedoms of data subjects (a requirement of a measure's appropriateness according to the Article 25 Guidelines), but because it was the most expedient measure to achieve functionality of the modified Video Uploader feature.

131. MPIL stated:

The developer selected the FB4A app ID because he knew that the Upload Service already worked successfully with Facebook for Android. Moreover, when the developer tried other app IDs (e.g., an app ID associated with a web composer), the Video Uploader failed to function properly. While the developer made a note in the code that a new app ID should be developed for the Video Uploader Token before it was launched, he was unaware of any security issue arising from the use of the FB4A app ID for the Video Uploader, and no change was ultimately made to the app ID for the Video Uploader Token before the upgraded Video Uploader was launched to the public in August 2017.⁷⁶

132. The DPC has been provided with a number of documents referred to by MPIL as 'diffs'⁷⁷ and 'tasks'⁷⁸ which record the coding process of the Video Uploader and attempts made by Meta engineers to review and change the code in responding to identified objectives before its launch to the public.⁷⁹

133. Specifically the developer stated on 16 June 2017 in the Video Uploader code diff 'I am going to find the appropriate app. Was just testing using this'⁸⁰ and stated later in the

⁷⁵ MPIL Response 14 March 2019 (Processor Inquiry), 4.

⁷⁶ MPIL Response 14 March 2019 (Processor Inquiry), 4-5. Emphasis added.

⁷⁷ MPIL described a diff in respect of its software development controls as follows: 'To initiate a change to the Facebook codebase, a change author must create a "differential," or "diff," which describes the proposed change. All reviews and tests of the new code are automatically logged in the diff throughout the development process.' See Response to First Queries, 22.

⁷⁸ MPIL described a task in the related Processor Inquiry as 'a form of documentation typically used to identify and track work needed on a non-urgent security issue'. See MPIL Response 14 May 2019 (Processor Inquiry), 6. The DPC understands a 'task' to be a computing term describing a document containing a piece of work to be undertaken by assigned developers at Meta in order to bring about a result (e.g. such as to remedy an identified vulnerability). It appears that a number of diffs may be created in addressing an associated task.

⁷⁹ The DPC was provided with 'diff' and 'task' documents relevant to the coding of the Video Uploader and the access token by Meta in the associated Processor Inquiry. MPIL provided duplicates of some of those documents in this Inquiry.

⁸⁰ D5163264 -Introduce byte level resumability to www video uploads (created 1 June 2017), 5.

code [REDACTED]⁸¹ In another related diff the same developer states '[w]ill be creating a new app id before launching it to public.'⁸²

134. It appears that the access token was never intended to be used by the Video Uploader in a live environment, or even beyond testing, and the engineer tasked with writing the code to generate the access token made it clear that its use was inappropriate and should not be launched to the public. As such the DPC considers that MPIL knew or ought to have known that it should not have been used, notwithstanding MPIL's assertion that the engineers involved in coding the Video Uploader were unaware that the token carried 'any specific security implications.'⁸³
135. The DPC agrees with the inquiry team when they state in the Inquiry Report that access tokens carry enormous trust, due to their function as an authentication / authorisation mechanism, i.e. they confirm that the bearer of the token is who they claim to be , (i.e. that it is a 'bearer token'). As such, there is substantial risk associated with their use and potential account compromise. The DPC considers that any surface in a web application which handles authentication / authorisation should do so with the utmost scrutiny to mitigate that risk, in order to ensure that data protection by design and default has been fully considered and implemented. Given that mishandling of authentication and/or authorisation controls relating to user accounts could result in severe consequences for the user, such as a full account takeover, the DPC considers that authentication / authorisation is one of the most sensitive aspects of managing the security of a user's online account.
136. The access token was configured so as to carry full permissions in that it provided access to all user Facebook profile data through the Graph API. It could be used to obtain a session cookie to log into the user's Facebook account as that user and was non-expiring in nature. MPIL explained:

The specific type of token used for the video uploader carried full permissions to access the user's data through the Graph API, as attempts to substitute a more narrowly permissioned token had caused the video uploader not to work reliably;⁸⁴

The access token used by the video uploader was a fully permissioned, first-party access token. This means that it could be used to request from the Graph API essentially any data for a user that privacy settings allow the user to see on WWW.

⁸¹ D5163264 -Introduce byte level resumability to www video uploads (created 1 June 2017), 9.

⁸² D5500527 'OG_COMPOSER appID doesn't work for all users' (created 1 June 2017), 1.

⁸³ MPIL Submissions on the Inquiry Report, footnote 180.

⁸⁴ Response to First Queries, 14.

This data includes, among other things, all fields of a user's profile information;⁸⁵and

[T]he access token collected for a seed user's friend could be used to request a session cookie for the friend's account through the Graph API.⁸⁶

137. The DPC considers that there is significant risk associated with processing which relies upon the generation of an access token, where that access token is configured with extensive permissions to access personal data (as it was in this case), should that access token be improperly obtained and exploited by a bad actor.

138. MPIL should have provided a safeguard to this risk by limiting the permissions associated with the access token, in line with the purpose for which the token was created. This would accord with the commonly understood principle in Information Security of the 'principle of least privilege', which dictates that, in a given scenario, only the minimum privileges necessary to complete a given task should be assigned.⁸⁷ The principle closely aligns with the requirements of data protection by design pursuant to Article 25(1) GDPR and by default under Article 25(2), which states that controllers must ensure that 'by default, only personal data which are necessary for each specific purpose of the processing are processed'.

139. Further, the DPC agrees with the inquiry team in the Inquiry Report when they state:

Narrow scoping of the token so that it only provides the minimum access to personal data strictly necessary to perform its function and expires within the shortest necessary lifespan is essential and accords with the principle of data protection by design and default under Articles 25(1) and 25(2) GDPR, and the GDPR's principles of necessity, proportionality, data minimisation and purpose limitation.⁸⁸

140. MPIL argues in its submissions on the Inquiry Report that:

Meta Ireland is unaware of any established industry framework that would preclude an online service from issuing a fully permissioned access token to the user of the account to which the token provides access. Indeed, it is commonplace for a user to be provided with a fully permissioned credential, whether it be an access token or a session cookie, as a result of logging into their account. Without

⁸⁵ Post-mortem Incident Report, 2.

⁸⁶ Submissions on the Inquiry Report, para 6.3.

⁸⁷ OWASP Cheat Sheet Series 'Authorization Cheat Sheet' available at: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html (Retrieved 16 April 2024).

⁸⁸ Inquiry Report, para 287.

such a credential, a user cannot access all of the data and use all the available features in their account to which they are entitled.⁸⁹

141. MPIL asserts that the access token was appropriately configured to access the personal data necessary for what it was required to do. MPIL states '[t]he Video Uploader Token did not provide the receiving user with any greater privileges than they were supposed to have.' MPIL accordingly asserts that the 'principle of assigning users only the minimum privilege necessary to complete their job' is 'not relevant'.⁹⁰
142. The DPC accepts that there are circumstances where a fully provisioned access token may be issued to a user to permit authentication of further logins. However, such a token should never be issued to a third party and it was not appropriate to issue them in circumstances where it was intended to provide visibility of public data only. Producing such a fully provisioned access token created the risk of the access token being disclosed to an unauthorised party, thus compromising the user account associated with the credential. As the access token was *intended* to be issued only to a user who was already validly logged in, MPIL should have recognised the risk of invalid distribution of that token and implemented safeguards accordingly.
143. The DPC considers this scenario demonstrative of the necessity for MPIL to implement data protection by design and default in each component of the processing system, particularly where it is not clear where vulnerabilities can arise. In accordance with Article 25(1) GDPR, MPIL should have implemented effective safeguards in these circumstances where inherent risk associated with an authentication/authorisation mechanism actualises due to an unanticipated vulnerability. Those safeguards should serve to limit the surface of attack and limit the gravity and consequences of the risk materialising.
144. In addition, in accordance with Article 25(2) and the principle of data minimisation, the access token should have had access by default only to the minimum amount of personal data necessary to achieve each specific purpose, and effectively protect the rights and freedoms of its users. Article 25(2) also requires adherence to the principle of purpose limitation. EDPB states '[t]he controller should choose and be accountable for implementing default processing settings and options in a way that only processing that is **strictly necessary** to achieve the set, lawful purpose is carried out by default.'⁹¹
145. The DPC considers that the access token was over-permissioned in its design and by default, in so far as such a generated token:
- (1) did not require full access to all the user's profile personal data available from the Graph API;

⁸⁹ Submissions on the Inquiry Report, para 14.5.

⁹⁰ Submissions on the Inquiry Report, para 14.6.

⁹¹ Article 25 Guidelines, para 42. Emphasis added.

- (2) did not require functionality to generate a session cookie from the Graph API; and
- (3) did not need to be non-expiring to achieve its purpose.
146. The DPC considers points (1) and (2) in the preceding paragraph aggravated the gravity and severity of the Breach. Arising from point (1) whole categories of personal data such as location information, email addresses and telephone numbers were rendered vulnerable to attack, and were needlessly affected by the Breach. Save for point (2), the vulnerability would not have been able to propagate as it did, and the attack (and the affected users) would have been limited to the friend list of the initial 'seed' account.
147. In light of the above considerations, the DPC rejects MPIL's submission that the '[v]ulnerability was not caused by any technical or organisational weakness in the sense of a lack of appropriate security measures or controls.'⁹²
148. Although the non-expiring nature of the access token's design and continued use during the relevant period presented a security risk in itself, the DPC accepts MPIL's position that it was not a factor in the Breach. MPIL stated:

We note that the expiry properties of the Video Uploader Token were not a factor in the Attack, as the tokens generated as part of the Attack were promptly used by the attackers thereafter (typically within minutes) to obtain data from the corresponding user accounts through the Graph API. Moreover, all of these tokens were invalidated as part of the remediation of the Attack.⁹³

149. Although the non-expiry of the access token was not exploited in the Breach, the attacker had possession of the tokens for the duration of the attack, and therefore the ability to impersonate the affected users indefinitely until the Breach was detected and remediated, and the tokens were invalidated. This created a severe risk (although unrealised) of further account takeovers of third-party applications that rely on Facebook's single sign-on function (a session and user authentication service that permits users already authenticated by Facebook to access multiple applications).
150. In light of the above, the DPC does not consider that MPIL has verified the appropriateness of the measures for the particular processing in question, as the EDPB explicitly notes is required for compliance with Article 25.⁹⁴
151. The DPC considers that MPIL could have implemented appropriate measures to ensure that, by default, the access token generated by the Video Uploader feature processed

⁹² Submissions on the Inquiry Report, para 4.9.

⁹³ Response to Third Queries (8 April 2019), 7.

⁹⁴ The EDPB states '[s]tandards, best practices and codes of conduct that are recognized by associations and other bodies representing categories of controllers can be helpful in determining appropriate measures. However, **the controller must verify the appropriateness of the measures for the particular processing in question.**' (Emphasis added) See Article 25 Guidelines at 6.

only personal data that was necessary for its specific purpose of processing. Such measures could have included limits on the permissions that the access token carried to access data through the Graph API, restrictions on the ability to generate a session cookie, and a restriction on the non-expiring nature of the token. The DPC considers that such measures could have ensured that only personal data which were necessary for the purpose of the processing were processed, as required by Article 25(2) GDPR.

152. The DPC also considers that alternative measures to permit users to resume video uploads in the event of disruption or disconnection could have more effectively implemented the integrity and confidentiality principle as required by Article 25(1) GDPR. The use of the access token introduced an unnecessary attack vector, and lacked in safeguards to ensure the confidentiality of the personal data.

ii. Design impact of the access token on Logging, Incident Alerting and Detection

153. MPIL define app ID as being ‘the identifier of the specific application associated with the access token.’⁹⁵ MPIL further explain the purpose of the app ID is to act as an identifier for its internal processing, by stating that it is ‘intended to reflect the type of application that the token was being generated for.’⁹⁶
154. Accordingly, MPIL outlined that in the development process, efforts were initially made to use an app ID which specifically referenced the Video Uploader. However, issues were encountered by the developer when trying to implement the intended access token, which would have correctly labelled the token as one relating to the Video Uploader. Ultimately, as already stated, the app ID which was used for the Video Uploader was the app ID for the Facebook application on Android app ID (the FB4A app ID). The FB4A app ID is generally associated with the Facebook application on Android (mobile) operating systems, and not the web platform upon which the Video Uploader appeared.
155. The DPC considers that the design and specification of the FB4A app ID access token used by the Video Uploader made it difficult for Meta to distinguish between tokens generated as a result of malicious activity and activity relating to existing and newly generated Android sessions. The attack involved a spike in user growth metrics (particularly ‘an anomalous spike in activity among users that had been inactive for at least 30 days’)⁹⁷ and the generation of millions of access tokens. Because the FB4A access token was used, the anomalous spike in activity among users (indicating the beginning of the attack), appeared to relate to already-existing and newly generated sessions on Android, and accordingly, the statistics were surfaced ‘as part of its routine work validating user metrics’ to the Meta’s Growth Team,⁹⁸ which MPIL submitted is

⁹⁵ Response to Third Queries (8 April 2019), 6.

⁹⁶ MPIL Response 14 March 2019 (Processor Inquiry), 4.

⁹⁷ Post-mortem Incident Report, 5

⁹⁸ Post-mortem Incident Report, 5.

‘responsible for various initiatives to grow and monitor the Facebook user base’,⁹⁹ and which has no specific security related function. MPIL submitted that ‘user growth patterns generally have nothing to do with security vulnerabilities’, and for security personnel to monitor all these metrics directly ‘would result [in] signal overload’ and would not be an ‘efficient use of resources.’¹⁰⁰

156. MPIL submitted that it was upon observing a spike in user growth metrics that Meta’s Growth Team was led to investigate. However, it stated that the Growth Team

had no reason to believe that it reflected any malicious activity, let alone a large-scale attack. The Growth Team instead believed the activity might be the result of a new app that was not making correct API calls or was not being logged correctly.’¹⁰¹

157. While a spike in login activity might rationally have been explained by the popularity of a new app or a ‘localised event that causes a temporary increase in user traffic in a particular country or region’,¹⁰² if the appropriate app ID had been used to signify that the token generation specifically related to the Video Uploader, suspicion would likely have been aroused as to why so many users were seeking to upload a video at the same time at a rate of millions of instances above normal usage (as a correctly labelled version of the access token would have indicated). In the circumstances, the access token was not correctly labelled and the spike in activity was not initially suspected by MPIL as suspicious.
158. In the related Processor Inquiry, Meta advised the DPC that its security team ProdSec¹⁰³ identified that the use of the FB4A app ID could appear misleading in its logs, in that activity from the Video Uploader would appear to be from Android usage even though it was occurring on the web platform.¹⁰⁴
159. The DPC considers the labelling of the Video Uploader tokens as access tokens for Android impacted MPIL’s ability to accurately monitor the tokens that were being generated by the Video Uploader during the attack.

⁹⁹ Submissions on the Inquiry Report, para 7.2.

¹⁰⁰ Submissions on the Inquiry Report, para 16.18.

¹⁰¹ Submissions on the Inquiry Report, para 7.3.

¹⁰² As suggested by MPIL. See Submissions on the Inquiry Report, para 16.24.

¹⁰³ ‘ProdSec’ refers to Meta’s Product Security Team, which MPIL advised the DPC is responsible, *inter alia*, for identifying and fixing vulnerabilities in Meta’s product code.

¹⁰⁴ MPIL Response 14 March 2019 (Processor Inquiry), 5.

160. In terms of timeline, the attack commenced on Friday 14 September 2018,¹⁰⁵ the spike in activity was detected and investigated by the Growth Team on Monday 17 September 2018, but it was not until Tuesday 25 September 2018 – after the Growth team had determined that ‘much of the activity was stemming from a single IP address’¹⁰⁶ – that Meta’s formal incident response procedures were engaged when the Growth Team escalated the matter to Meta’s security on-call personnel for investigation at approximately 8:00 a.m. (US Pacific Daylight Time). MPIL stated:

The security engineers soon determined that the spike in activity was due to an attack in which the attackers were somehow generating access tokens for other accounts while in View As mode. By 11.00 on 26 September 2018, a security engineer was able to fully uncover the precise mechanism involved in the Vulnerability.

Upon discovering the root cause of the Vulnerability, engineers promptly began developing a remediation plan, which was fully executed in less than 48 hours.¹⁰⁷

161. While the DPC commends MPIL for its prompt and effective remediation efforts *after* its formal incident response procedure was engaged (it took Meta eleven days from the commencement of the attack to determine that an attack was in progress and thereafter three days to remediate the conditions of the vulnerability which gave rise to the Breach), it considers that MPIL’s monitoring and logging measures could not operate effectively when the access tokens were not logged using an appropriate label, and when the logging and monitoring measures in place did not flag or suspend suspicious activity associated with a spike in user activity that affected millions of users and largely emanated from a single IP address. Appropriate logging and monitoring would have facilitated a more prompt engagement of its incident response measures.
162. The DPC accepts that the Breach was detected as a result of investigation into an anomalous spike in the number of ‘resurrected users’ (i.e. users returning to activity after more than 30 days’ absence.) The DPC also accepts that there are many innocent reasons (such as the use of VPNs or proxies) that may account for spikes in traffic from individual IP addresses. However, the DPC finds that a properly labelled app ID showing the use of an over-permissioned access token from a single IP address would have enabled a more prompt and specific identification of the cause, nature and effect of the Breach. The DPC accordingly does not accept MPIL’s submissions that the mislabelled app ID had no effect on the ability to detect the Breach.¹⁰⁸

¹⁰⁵ MPIL state ‘...we believe that the attack which led to token being inappropriately accessed, commenced on 14 September 2018, because we discovered (on 26 September 2018) that an unexpected spike in ‘View As’ traffic began on that date.’ See Update to Cross-Border Breach Notification Form, 13.

¹⁰⁶ Post-mortem Incident Report, 5.

¹⁰⁷ Submissions on the Inquiry Report, para 7.5.

¹⁰⁸ MPIL Submissions on PDD, 7 February 2023, para 8.31- 37.

163. The Open Web Application Security Project ('OWASP') noted 'Insufficient Logging and Monitoring' as one of the top 10 application security risks in its 2017 edition, which recommends: 'As per the risk of data stored or processed by the application establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.'¹⁰⁹
164. The DPC considers the design of the access token for mobile use and its application for web-used use resulted in 'mislabelling' of the access token, which negatively affected visibility and incident alerting, and likely contributed to a delay in the detection the attack, the escalation of the matter to the appropriate security team and accordingly the remediation of the Breach. The DPC considers that alternative appropriate measures for monitoring and logging, including the use of appropriate labelling, could have more effectively implemented the integrity and confidentiality principle as required by Article 25(1) GDPR. However, MPIL failed to implement such measures during the temporal scope.
- iii. **Regular reviews and assessments of the effectiveness of the chosen measures and safeguards**

(a) Risk reviews

165. Appropriate technical and organisational measures in connection with the processing subject to the Breach should properly involve a risk assessment framework, in accordance with Article 25 GDPR.
166. This framework must be directed to compliance with the GDPR, and should require ongoing, regular and comprehensive risk assessments and reviews throughout the lifecycle of the processing in recognition that risks are not static and in order to demonstrate measures remain appropriate. The risk reviews must consider new and emerging risks, particularly where software modifications are made.
167. Accordingly, the DPC agrees with the inquiry team when they state in the Inquiry Report that MPIL should have 'developed a methodology for the calculation and recalculation of risk(s) associated with the processing and that its application of that methodology would have meaningfully contributed to the ongoing implementation, maintenance, and improvement'¹¹⁰ of its measures. The DPC considers that MPIL was required to demonstrate and provide the DPC with documentation evidencing this methodology and its associated regular risk assessments and reviews in respect of the processing subject to the Breach in accordance with its obligations pursuant to Article 25 GDPR and in order to verify the effectiveness of its measures.

¹⁰⁹ OWASP 'A:102017- Insufficient Logging & Monitoring', available at:

https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging&Monitoring

¹¹⁰ Inquiry Report, para 172.

168. In respect of a controller's obligation to carry out risk assessments, the EDPB stated the following:

The GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing).

When performing the risk analysis for compliance with Articles [sic] 25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments.

...

...controllers...**must always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed.**¹¹¹

169. MPIL stated that it did not carry out a risk assessment, or a manual security review of the modification to the Video Uploader to generate fully permissioned access tokens in July 2017, or subsequently from 25 May 2018, from which time MPIL was required to discharge its obligations under the GDPR.

170. MPIL submitted:

It is not practical to expect similarly formal risk assessments to be prepared before every code change, nor does GDPR require any such practice...there is always a risk that unknown, unforeseen bugs may be introduced by a code change. That is a background risk of coding that does not need to be restated in a formal risk assessment every time a code change is made.¹¹²

¹¹¹ Article 25 Guidelines, 9-10. Emphasis added.

¹¹² Submissions on the Inquiry Report, para 13.14.

171. The DPC considers that every time a piece of software is changed or developed, the controller should ensure that the developer takes into account Article 25 GDPR and the risks that may be presented to the existing codebase by the introduction/modification of a particular feature. As already stated, the coding of the Video Uploader occurred prior to the GDPR coming into force, is outside the temporal scope of this Inquiry, and does not fall to be considered in this Decision.
172. In its submissions on the PDD, MPIL argued that, as the introduction of the Video Uploader Token and associated issues concerning documentation and training all occurred before the entry of the GDPR into force on 25 May 2018, findings in this Decision concerning them 'are not within the Temporal Scope [of the DPC's inquiry] and should therefore not influence the DPC's decision.'¹¹³
173. However, as already stated, the EDPB has interpreted Article 25 to require that a controller must re-evaluate their pre-GDPR processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards. The EDPB states:
- The obligation to maintain, review and update, as necessary, the processing operation also applies to pre-existing systems. This means that legacy systems designed before the GDPR entered into force are required to undergo reviews and maintenance to ensure the implementation of measures and safeguards that implement the principles and rights of data subjects in an effective manner, as outlined in these Guidelines.¹¹⁴
- This obligation also extends to any processing carried out by means of data processors. Processors' operations should be regularly reviewed and assessed by the controllers to ensure that they enable continuous compliance with the principles and allow the data controller to fulfil its obligations in this respect.¹¹⁵
174. Accordingly, the DPC considers that MPIL's measures during the temporal scope ought to have included assessing its pre-existing measures, carrying out regular risk assessment(s) into the modification of the Video Uploader, and assessing the security risks associated with its use of fully permissioned access tokens after GDPR came into force in May 2018 and during the temporal scope. MPIL was obliged to provide supporting documentation demonstrating that those risks were addressed in a way that specifically relates to its processing systems. The DPC expects such documentation to be clear, comprehensive and robust. The DPC agrees with the inquiry team in the Inquiry Report when they state 'absent a comprehensive understanding of the risk(s) associated with the processing, [MPIL's] capacity to identify, assess, manage, and respond to extant

¹¹³ MPIL Submissions on PDD, 7 February 2023, para 8.4.

¹¹⁴ Article 25 Guidelines, para 38.

¹¹⁵ Article 25 Guidelines, para 39.

and emerging risk(s) by implementing further measures would be limited.’¹¹⁶ The DPC considers that MPIL has failed to provide the DPC with any such documentation, or demonstrate that risk assessment(s) were carried out.

175. MPIL submitted, in its submissions on the Inquiry Report and in various replies to the DPC’s queries during the Inquiry, that the Breach was caused by an ‘obscure interaction of three distinct Facebook features’, ‘not intended or anticipated to be used together’, that the vulnerability was ‘complex and novel’, and that the risk was ‘not reasonably foreseeable.’ MPIL asserted that the GDPR does not require organisations ‘to assess risks emanating from bugs that are not known or reasonably foreseeable at the time when every code change is made.’¹¹⁷
176. The DPC considers that any implementation of an authorisation/authentication token should take into account the inherent risks associated with using a bearer token that provides the holder of the token with the ability to carry out any action with which the token is permissioned. Taking into account this inherent risk, it would not be necessary for MPIL to foresee a complex combination of events occurring (as MPIL has argued). Instead, MPIL should seek to limit the impact of the inherent risk and reduce the risk of unauthorised disclosure. Any risk assessment should have taken this inherent risk into account and treated that risk appropriately. In accordance with Article 25(1) and (2) a risk assessment should identify and consider each distinct and granular risk inherent in the layers of the processing’s design which may or may not combine or contribute to form a greater risk.
177. In its Submissions on the PDD, MPIL argued that the DPC’s view of appropriate security standards were unrealistic and went beyond those required by the GDPR generally and Article 25 in particular:

[T]he PDD appears to take the position that MPIL was required to conduct *formal, manual* reviews of all ‘legacy systems designed before the GDPR entered into force,’ including the Video Uploader Token. [...]

However, the expectation that a controller of *any* large online platform, let alone one the size of the Facebook service, could or should conduct regular manual security reviews of every single feature in its codebase, each reflected in formal documentation, is impracticable.¹¹⁸

178. The DPC does not accept this argument. The GDPR does not prescribe ‘formal manual reviews’, nor does the DPC’s understanding of its application to the present case suggest that MPIL should have conducted such reviews of ‘every single feature in its codebase’. The GDPR sets standards by reference to risk, and the technical and organisational

¹¹⁶ Inquiry Report, para 173.

¹¹⁷ Submissions on the Inquiry Report, para 13.14.

¹¹⁸ MPIL Submissions on PDD, 7 September 2023, para 8.6. Emphasis in original.

measures required to meet those standards must reflect risks in terms both of the degree of scrutiny required and the priority that controllers should assign to addressing them.

179. At a minimum, MPIL's risk assessment(s) during the temporal scope should have identified the high risks associated with using fully permissioned access tokens and measures appropriate to mitigate that risk by identifying if an appropriate alternative mechanism for authorisation carrying less risk to the rights and freedoms of its users could be implemented instead.
180. Given that the Video Uploader was designed to generate a fully permissioned access token, which, if mishandled, could result in full account takeovers of affected data subjects, a risk assessment should have also identified all existing Facebook features that the Video Uploader could interact with. This would include all cases where the Video Uploader could have appeared as part of the Birthday Composer, and assessed the risks associated with those features and their usage of the token, subsequently implementing appropriate measures and safeguards to mitigate this risk.

(b) Security reviews and assessments

181. In accordance with Article 25(1) GDPR, MPIL is obliged to ensure, and to demonstrate that regular security reviews and assessments of the effectiveness of its measures and safeguards have been carried out in order to demonstrate the measures' appropriateness. This is closely connected with risk reviews.
182. MPIL stated that Meta's Product Security Team ('ProdSec') which sits within its detection and security infrastructure group, is responsible for identifying and fixing vulnerabilities in its product code, and conducts hundreds of manual security reviews of products.
183. MPIL explained:

ProdSec personnel work with product teams in the development stages of 'designated projects', which are designated based on broad security priorities identified by ProdSec or requests by product teams. Learnings from these reviews are then used to continually update the sophisticated automated tools, to ensure that all Facebook code is checked for known types of vulnerabilities prior to launch.¹¹⁹

184. MPIL submitted that no manual security review of the Video Uploader was carried out at the time it was modified in July 2017, as it was not a new Facebook product. MPIL stated that it was 'merely an upgrade to a pre-existing Facebook product and was not specifically designated for a manual security review at the time.'¹²⁰

¹¹⁹ Submissions on the Inquiry Report, para 15.3.

¹²⁰ Submissions on the Inquiry Report, para 15.4.

185. Thereafter, MPIL did not carry out, and has failed to demonstrate that any security review or audit of Meta's use of access tokens was carried out either by MPIL, by Meta's security personnel or at all during the temporal scope. MPIL stated:

[MPIL] did not instruct/conduct a review and/or audit of FB Inc.'s use of access tokens between 12 July 2017 to 28 September 2018;¹²¹ and

[REDACTED]

[REDACTED]¹²²

186. Further MPIL stated it [REDACTED]

[REDACTED]¹²³

187. The DPC considers that given that no security or risk assessment was performed into the new usage of the token during the temporal scope, appropriate mitigations for the risk posed by the new processing operation and necessary safeguards could not be identified and implemented.
188. MPIL did not carry out a manual review into the modified Video Uploader during the temporal scope, as part of its ongoing obligation to regularly review and assess the appropriateness and effectiveness of its measures and safeguards pursuant to Article 25(1) GDPR.
189. Meta was made aware of certain security risks associated with the access token via the receipt of a report through its bug bounty programme¹²⁴ in October 2017, which it stated prompted ProdSec to carry out a review of the Video Uploader's code.¹²⁵
190. MPIL stated:

...in October 2017, a bug bounty report was received through the white hat program that, while not expressly about the Video Uploader Token, led ProdSec to review the code for the Video Uploader Token in December 2017. Through that

¹²¹ Response to Third Queries (26 April 2019), 17.

¹²² Response to Third Queries (26 April 2019), 21.

¹²³ Response to Third Queries (26 April 2019), 17.

¹²⁴ The bug bounty programme is described by MPIL as a measure which incentivises external security experts to search for and report any bugs discovered in the Facebook service. Reports received through the bug bounty program ('white hat' reports) are triaged by the ProdSec team based on the level of risk they present and are then directed to the appropriate teams for validation, investigation and resolution. See 10-17-18 Whitehat Report 1523279721051701.

¹²⁵ The report identified two issues with the FB4A token affecting the Meta Workplace Product, being: the persistence of the access token after account deactivation, and the access token was non-expiring. In the course of investigating the report, ProdSec identified that the same FB4A tokens were being used by the Video Uploader. See 11-23-18 Whitehat Report 1565865740126432.

review, ProdSec identified certain security risks concerning the Video Uploader Token, and worked with the product team to mitigate these risks. ProdSec reasonably assessed this issue as non-urgent, as it did not present any vulnerability that, by itself, could be used to compromise another user's account. The issue proved difficult to fix and remained open at the time of the Attack.¹²⁶

191. MPIL submitted that ProdSec identified the risks that the access token was non-expiring; and that should a user's access token become compromised, it granted full access to all user data obtainable through the Graph API. As stated previously, this latter risk was a factor involved in the Breach.

192. MPIL stated in the associated Processor Inquiry:

ProdSec identified two risks associated with the Video Uploader Token and raised these risks with the product team. First, ProdSec assessed that the use of the FB4A app ID could appear misleading in Facebook's logs, in that activity from the Video Uploader would appear to be from Android usage even though it was occurring on the web platform. Second, the FB4A app ID carries full API permissions, meaning that a token with this app ID provides full access to the data in a user's account. ProdSec assessed that the use of a fully permissioned token for the Video Uploader entailed a risk that, if such a token were obtained by an attacker from a user's account, it could be used to silently persist access—i.e., to continue controlling the account even if the original means of access were terminated.¹²⁷

193. In the associated Processor Inquiry, MPIL was requested to provide the DPC 'with the specific assessment conducted, in original form by the ProdSec team who identified the two risks associated with the Video Uploader Token.'¹²⁸ In response, MPIL sought to rely on a 'task' document, entitled '[Workplace] Access tokens is still valid after 'Set to Unclaimed' or 'Log out everywhere' (task no. T23978891), by stating:

Please see T23978891, the task created in response to the bug bounty report that led ProdSec to identify the two risks at issue, which was cited in and attached to the March Response. A task would be the form of documentation typically used to identify and track work needed on a non-urgent security issue. In particular, please see the December 7, 2017 comment in T23978891 from [name of Meta employee], a ProdSec engineer, in which the two risks are identified.¹²⁹

194. This document (task no. T23978891) appears to show comments made by various personnel in Meta discussing issues with the access token amongst themselves in an

¹²⁶ MPIL Response 14 March 2019 (Processor Inquiry), 4.

¹²⁷ MPIL Response 14 March 2019 (Processor Inquiry), 5.

¹²⁸ DPC Queries 2 April 2019 (Processor Inquiry), question 5(a), 8, and also MPIL Response 14 May 2019 (Processor Inquiry), 6.

¹²⁹ MPIL Response 14 May 2019 (Processor Inquiry), 6.

unstructured and informal way. The comment by a ProdSec engineer on 7 December 2017 which MPIL asserts identifies the two risks is as follows:

Slightly related, but these access tokens appear to be related to the Uploader service. [REDACTED] suggests this shouldn't be launched to the public (and I would agree, using an [REDACTED] token for FB4A here appears misleading at best and at worst is an easy way to silently persist access as an attacker). [Name of Meta engineer colleague], what's going on with this? Can we use a different app ID here?¹³⁰

195. The DPC does not accept that this document represents or demonstrates that a risk or security review assessment was carried out into the use of the access token by the Video Uploader, or that the code of the Video Uploader was regularly reviewed and assessed in a manner directed to compliance with Article 25(1) GDPR. As MPIL confirmed (in the quote within paragraph 193 above), this task document is 'the form of documentation typically used to identify and track work needed on a non-urgent security issue', and is not intended to be a security assessment. While the DPC notes that the date the relevant comment was made (December 2017) precedes the temporal scope of this Inquiry, MPIL has submitted that Meta was working to mitigate the risks identified therein during the temporal scope. MPIL stated:

Notwithstanding the limited risk understood to be presented by its use, the Upload Client team made substantial efforts to resolve the issues with the Video Uploader Token. Those efforts did not result in a solution being found, however, and the work remained an ongoing project as at the time of the Attack in September 2018.¹³¹

196. As such, this document falls to be considered by the DPC as relevant to MPIL's obligations under GDPR. The DPC considers the deficiencies of this document include, but are not limited to, its failure to:
- 1) record a regular assessment;
 - 2) record the scope and methodology for the assessment;
 - 3) identify the inherent risks associated with using authorisation/authentication tokens;
 - 4) consider or refer to best practice or a framework for implementing FB4A tokens in the Facebook service;
 - 5) identify the risk associated with the access token having full access to all user profile data on the Graph API;
 - 6) consider data accessibility limits at the point of design;

¹³⁰ T23978891 – '[Workplace] Access token is still valid' (created 29 November 2017), 2. Emphasis added.

¹³¹ Submissions on the Inquiry Report, para 5.10.

- 7) demonstrate that all attack vectors for authorisation/authentication tokens were considered;
 - 8) consider or refer to best practice or a framework for implementing FB4A tokens in the Facebook service;
 - 9) contain recommendations;
 - 10) assign individuals to work on, and determine a timeframe to mitigate the risks; and
 - 11) demonstrate how the risks were determined as non-urgent.
197. MPIL submitted that ProdSec assessed the most significant risk from the Video Uploader access token as being the potential for an attacker to persist access. MPIL submitted that the use of a fully permissioned access token by the Video Uploader 'did not by itself enable an attacker to obtain access to a user's account'¹³² and that some other means was required to effect an account compromise. It stated that the risk was viewed as one of 'defence-in-depth,' and was therefore assessed by Meta as being non-urgent. Contemporaneous evidence of this assessment has not been provided to the DPC.
198. The DPC has considered the Export Report of Professor Siegel, who argues similarly on behalf of MPIL that:
- the risk assessment made by the Product Security team was reasonable in light of what was known at the time. It was only the unknown interaction of the Video Uploader with the other two features involved in the Vulnerability that allowed access to another user's access token and thus presented an account compromise vulnerability. Again, because this feature interaction was not anticipated at the time, there was no reason to assess the risk from the Video Uploader Token any differently.¹³³
199. The DPC accepts that in the circumstances of the Breach, the attack necessitated the exploitation of the Vulnerability (arising from the interaction of three features carrying three discrete bugs), in order for the attacker to obtain the access tokens and carry out the attack. However, irrespective of whether the attacker required some other means in order to obtain the access tokens, the design and ongoing processing by the Video Uploader of the flawed access tokens created a security weakness and introduced an additional unnecessary surface vector carrying a high risk associated with the possibility of account takeover due to the capabilities of the access token, which should have been identified by a risk assessment during the temporal scope. Just because the attack relied upon the vulnerability to exploit the access tokens, does not diminish MPIL's obligation to ensure every layer of its design measures is appropriate, supported by risk

¹³² Submissions on the Inquiry Report, para 5.8.

¹³³ Expert Report, 12.

assessments and only permits access by default to such personal data necessary to achieve a given functional purpose.

200. This is also in keeping with the spirit underpinning MPIL's layered 'defence-in-depth' approach to security, where MPIL submits it applies multiple layers of security controls at different stages of the software development lifecycle that are designed to prevent, detect and fix software bugs.¹³⁴
201. Arising from the ProdSec assessment, MPIL states 'in December 2017, ProdSec recommended the creation of a new app ID, with narrower permissions to be associated with it, to be used for the Video Uploader.'¹³⁵ MPIL seeks to rely for this on the document named 'task no. T23978891' in which a ProdSec engineer asked on 7 December 2017 'can we use a difference app ID here?'). The DPC considers this document insufficient to demonstrate a recommendation of narrower permissions and has seen no further documentation evidencing such a recommendation beyond the engineer's suggestion of using a different app ID.
202. Whether or not ProdSec can be shown to have recommended creation of a new app ID with narrower permissions, no such recommendation was implemented and the access token continued to be used, despite the clear deficiencies in security identified by ProdSec, up until the remediation of Breach in September 2018.
203. MPIL stated:
- The Upload Client team within the Video Infrastructure group (which is responsible for building code libraries for the Video Infrastructure group) worked on this issue over the ensuing months, in consultation with ProdSec. However, the Upload Client team ran into repeated engineering difficulties in trying to implement ProdSec's recommendation. Attempts to substitute a different or more narrowly permissioned app ID for the Video Uploader Token continued to cause the Video Uploader not to work reliably.¹³⁶
204. The DPC has been provided with certain documentation ('tasks' and 'diffs') that records Meta engineers' comments in the code while working to implement what MPIL describes as ProdSec's recommendation 'to replace or modify the access token'.¹³⁷ On 14 April 2018, in the work task entitled 'Use separate AppID on composer instead of Facebook for Android' a Meta ProdSec engineer acknowledges that the access token is too highly permissioned. He states 'You don't want to blindly clone capabilities: the problem here was, in part, that you were using an access token that was too highly permissioned.'¹³⁸ On 21 May 2018 another Meta engineer questions whether the FB4A

¹³⁴ Submissions on the Inquiry Report, para 3.3.

¹³⁵ Submissions on the Inquiry Report, para 5.6.

¹³⁶ MPIL Response 14 March 2019 (Processor Inquiry), 6.

¹³⁷ As stated MPIL at Response to Fourth Queries, 2.

¹³⁸ T25932781 'Use separate AppID on composer instead of Facebook for Android' (created 9 February 2018), 4.

AppID is appropriate in the related task entitled 'Logout doesn't invalidate FB4A access token', asking 'Why do we generate a FB4A access token on a web session?'¹³⁹

205. Notwithstanding that the developer who coded the access token for the Video Uploader had not intended the access token to launch to the public, Meta was aware and/or ought to have been aware of certain risks with the access token (as identified by ProdSec) since December 2017. Although a ProdSec engineer attempting to remedy the risks in December 2017 agreed that it should never have been launched to the public (see query from the ProdSec engineer quoted at paragraph 201 above), the Video Uploader was permitted to continue to operate live and unchanged during the temporal scope until the occurrence of the Breach.
206. For the reasons set out above, the DPC finds that MPIL failed to carry out an appropriate risk or security assessment involving a case-by-case analysis of the risk arising from its chosen design, as recommended by the EDPB Guidance quoted above.
207. The DPC considers that the risk reviews and security reviews and assessments should have more effectively implemented the integrity and confidentiality principle as required by Article 25(1) GDPR. However, MPIL failed to implement such measures during the temporal scope.

(c) Alternative more appropriate measure

208. Shortly after the Breach, on 28 September 2018, a Meta engineer engaged in remediation efforts is recorded querying why access tokens are being used by the Video Uploader; the engineer was of the view that session cookies are a more appropriate means of authentication/authorisation. In the task titled '*Use separate app ID on composer instead of Facebook for Android*' (no. T25932781), the engineer asks:

Why are we using access tokens at all here? [REDACTED]

The response by another engineer is that the code only supported authorisation through access tokens, due to '[l]ack of support for understanding session cookies'.¹⁴⁰

209. The web-based Video Uploader's irregular use of access tokens (which were intended for mobile use) is evident from MPIL's submission that the Facebook website is coded using the programming language 'Hack', and that [REDACTED] within Hack', whereas the Facebook for Android mobile app is

¹³⁹ T29535827 'Logout doesn't invalidate FB4A access token' (created 18 May 2018), 9.

¹⁴⁰ T25932781 'Use separate AppID on composer instead of Facebook for Android' (created 9 February 2018), 2.

written in the different programming language C++ and [REDACTED]¹⁴¹ MPIL state:

At the time of the project to update the Video Uploader, a byte-level resumable video upload service was already in place for Facebook mobile apps, which was written in C++. For technical reasons, the language used to code the Facebook website – Hack – is not well-suited to process commands that require long processing times, which would include the upload of large files. Accordingly, the modification made to the Video Uploader in July 2017 involved modifying the Video Uploader so that it could utilise the same back-end video upload service already in place for Facebook mobile apps.

This existing back-end service relied on access tokens for authentication, as opposed to browser session cookies which are generally relied on for authentication within Hack.¹⁴²

210. MPIL further explained the reason why the access token was used:

Because of the role of the resumable video upload service in processing large data files, which is not what Facebook’s programming language for its website code (i.e. Hack) is designed for, the service is written in a different programming language and did not have existing code support for integrated cookie-based authentication. The engineers working on the Video Uploader Token prior to the Attack understood that creating a method for the resumable video upload service to support cookie-based authentication would require substantial work from multiple teams beyond the Video Uploader and ProdSec teams – as was in fact required when this change was implemented after the Attack.¹⁴³

211. MPIL provided the DPC with Meta’s post-mortem Incident Report which explains the steps taken to investigate and remediate the Breach. The report notes that [REDACTED]

[REDACTED]¹⁴⁴ The report states:

The version of the video uploader used in the Attack was also taken offline as a precautionary measure on 2018-09-28, by rolling the feature back to an earlier version that did not provide byte-level resumability and did not involve the generation of an access token. Subsequently, a new version of the byte-level resumable video uploader was developed that [REDACTED]

¹⁴¹ Submissions on the Inquiry Report, paras 5.1 and 5.2.

¹⁴² Submissions on the Inquiry Report, paras 5.1 and 5.2.

¹⁴³ Submissions on the Inquiry Report, para 14.19.

¹⁴⁴ Post-mortem Incident Report, 9.

[REDACTED] which we began to roll out to users in November 2018. [REDACTED]

[REDACTED] [Emphasis added]¹⁴⁵

212.

[REDACTED]

213.

It appears from the above that [REDACTED]

[REDACTED]

[REDACTED] While the GDPR is not prescriptive on the exact type of technical and organisational measures a controller should implement to meet its obligations, MPIL must be able to demonstrate that its design and use of the access token (or session cookies, if same had been relied upon) were secure, effective and appropriate.

214.

A proper security assessment carried out during the temporal scope should have identified that an alternative, more effective authorisation measure carrying less risk to the rights and freedoms of its users could be implemented instead. For clarity, this is based on what was known, and/or what should have been known to MPIL during the temporal scope, and not on information that was only discoverable after the Breach or the conclusions of the post-mortem Incident Report.¹⁴⁶

215.

While the cost of implementation, and the work involved in modifying or replacing the access token, is one factor that is relevant to considering measures in the context of the obligation to implemented appropriate measures, this must be balanced with the risk of the processing and the obligation to have regard to the state of the art. As already stated, the DPC considers that MPIL has failed to carry out a case by case analysis of the risk arising from its chosen design. At no point during the temporal scope did Meta or MPIL carry out a robust risk assessment and security review identifying that the generation of the fully permissioned access token by the Video Uploader and then using it when triggered from the 'View As' mode was disproportionate, unnecessary, or there was a less invasive alternative means of effectively achieving its purpose while ensuring the necessary safeguards to the rights and freedoms of its users in accordance with Article 25(1) of the GDPR. ProdSec's security review in 2017 was not provided to the DPC (as stated the DPC does not consider that the task document reflects or demonstrates a proper security review addressed to GDPR), its recommendations were not implemented, and no further risk or security reviews were carried out during the temporal scope until after the Breach.

¹⁴⁵ Post-mortem Incident Report, 9.

¹⁴⁶ Submissions on the Inquiry Report, para 14.19.

216. The DPC considers that an alternative, more effective authorisation measure carrying less risk to the rights and freedoms of its data subject users could have been implemented by MPIL instead of the access token during the temporal scope. Such a measure could have more effectively implemented the integrity and confidentiality principle as required by Article 25(1) GDPR. However, MPIL failed to implement such a measure during the temporal scope.

(d) Secure coding, policies and training

217. Having regard to the risk assessed above, the DPC considers that appropriate measures that MPIL could have had in place included best practice policies, procedures and guidance in relation to the selection, secure coding and secure use of access tokens across Meta's various processing systems (to include the use of the FB4A access token by the Video Uploader), during the relevant period.
218. The DPC accepts the inquiry team's analysis in the Inquiry Report that the access token was effectively an authorisation mechanism to authorise a user or application to interact with the Graph API, and considers that certain basic high level principles of authorisation tokens should have been applied, irrespective of the authorisation token framework being used. MPIL should also be able to demonstrate that relevant staff had been appropriately trained in those policies and procedures.
219. The DPC notes that Recital 78, which assists in interpreting Article 25 GDPR, states:

In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.

220. The DPC requested MPIL to '[p]rovide Relevant Supporting Documentary Evidence demonstrating that appropriate documentation and training was available to, and used by, developers up to 12 July 2017 regarding the secure implementation of the access token and session cookie.'¹⁴⁷
221. In response MPIL submitted two internal 'Wiki' documents from Facebook's intranet respectively titled 'Authentication & Access tokens' and 'Configuring the Access Token', and described by MPIL as '[g]eneral documentation concerning the use and configuration of access tokens.'¹⁴⁸ The documents provide only high-level information and are not instructive on the secure use or configuration of the access token. MPIL provided no further evidence in the Inquiry of policies concerning best practice or training for the secure implementation of the access token relating to the temporal scope.

¹⁴⁷ Third Queries, question 6, 13.

¹⁴⁸ Response to Third Queries (18 April 2019), 1.

222. MPIL submitted:

There would not have been documentation available that was specific to the 'access token' used for the video uploader. The video uploader involved the bespoke use of a Facebook for Android access token based on unique issues the developers encountered in coding the video uploader. No pre-existing documentation would have addressed this specific application of access tokens.¹⁴⁹

223. MPIL has also stated in its submissions to the Inquiry Report 'that there was no pre-existing documentation or training that was directly responsive to the challenges encountered, precisely because those challenges were novel and had no standard, straightforward solution.'¹⁵⁰

224. The DPC has examined the information supplied by MPIL in the Inquiry and finds that MPIL did not have any guidance or policy on when access tokens should be used for different processing purposes or contexts on the Meta platform in consideration of the high risk they pose as an authentication/authorisation mechanism; or a secure coding framework dictating how they should be configured in terms of their scope, limitations, permissions, and expiry properties necessary for their purpose during the temporal scope.

225. MPIL asserts that '[t]he difficulties encountered in resolving the issue of the Video Uploader Token's permissions were not due to a lack of training or documentation. After ProdSec identified the issue, efforts to resolve it were guided by personnel who were experts in access tokens and their use within Facebook systems.'¹⁵¹

226. The DPC considers that this assertion is not supported by evidence. The absence of best practice procedures, policies and training is evident from the engineer who coded the Video Uploader stating in the code 'I am going to find the appropriate app. Was just testing using this' and thereafter the code was released to the public; the documented efforts and ultimate failure of Meta's engineers to remedy the deficiencies with the access token identified by ProdSec in December 2017, while allowing the access token to remain live until the Breach; and the confusion expressed by various Meta engineers (experts or otherwise), regarding best practice for authentication frameworks. For example a Meta engineer working on remedying the issues with the access token queried the best practice in regard to scoping of the access token by stating on 21 May 2018:

¹⁴⁹ Response to Third Queries (18 April 2019), 1-2.

¹⁵⁰ Submissions on the Inquiry Report, para 14.21.

¹⁵¹ Submissions on the Inquiry Report, para 14.1(c).

...assuming we do need to generate an access token to use [REDACTED]
what's the best practice to be followed expiration or invalidation of the token?¹⁵²

227. Another Meta engineer queried on 18 July 2018 'whether this is proper use of the authentication frameworks.'¹⁵³
228. As already stated, shortly after the Breach on 28 September 2018, a Meta engineer queried why access tokens were being used by the Video Uploader, and the response stated it was due to lack of support for understanding session cookies.
229. In its Submissions on the PDD, MPIL argues that the DPC's criticisms of MPIL's policies, procedures and guidance relating to matters concerning the Breach 'largely seems to concern an alleged lack of documentation to guide the initial coding of the Video Uploader Token, which is outside the Temporal Scope.'¹⁵⁴ Accordingly, MPIL maintains:

...even if the Video Uploader Token was initially configured without adequate supporting documentation or training (which MPIL does not accept), any such alleged deficiencies are not within the scope of the Inquiry.¹⁵⁵

The DPC does not accept this argument. The Temporal Scope began on 25 May 2018, when the GDPR took effect. The standards and obligations imposed by the GDPR from that date applied in the same way both to existing processing arrangements and to those created or revised after the date it took effect. Controllers such as MPIL were well aware of those standards and obligations, and the need to revise and update policies, procedures, guidance and – where circumstances required – coding to meet the standards and obligations.

230. The DPC notes that MPIL appears to have made efforts after the Breach to address the deficiency in best practice documentation and training in the secure use of the access token as part of its remediation measures. Meta outlines in its post-mortem Incident Report the following improvements:

We have consolidated and expanded security documentation for software engineers with regard to secure use of access tokens. The documentation covers when access tokens should be used in the Facebook code, how they should be generated, best practices for their use, and links to related documentation. The

¹⁵² T29535827 – 'Logout doesn't invalidate FB4A access token generated from FB Profile' at 8. This task document is specifically referred to by MPIL under the category of 'Access Token Efforts' relating 'to the October 2017 bug bounty report and certain associated efforts made by Facebook, Inc. ('FB Inc.') to replace or modify the access token used for the Video Uploader prior to the Attack ('Access Token Efforts')'. See Response to Fourth Queries, 2). This particular task document relates to attempts to remedy the non-expiry risk identified with the access token.

¹⁵³ This query was raised in respect of the task addressing the non-expiring nature of the access token. See T29535827 – 'Logout doesn't invalidate FB4A access token' (created 18 May 2018), 5.

¹⁵⁴ MPIL Submissions on PDD, 7 February 2023, para 8.25.

¹⁵⁵ *ibid*, para 8.26.

documentation is now published on Facebook's internal wiki, will be included in the future in the mandatory security training given to all incoming engineers, and will be linked to in any relevant alerts that fire as a result of automated scans conducted during code reviews.¹⁵⁶

231. While MPIL is to be commended for identifying and making efforts to remediate its lack of documentation and training following the Breach, the DPC cannot consider it relevant to its assessment of MPIL's security obligations during the temporal scope. Any improvement to its measures implemented after the Breach occurred is out of scope of this Inquiry in the DPC's assessment of MPIL's compliance with GDPR but will be addressed, insofar as relevant, in the section of this Decision setting out the DPC's decision on corrective powers in accordance with section 111(2) of the 2018 Act below.
232. The DPC considers that best practice policies, procedures and guidance in relation to the selection, secure coding and secure use of access tokens across Meta's various processing systems could have more effectively implemented the integrity and confidentiality principle as required by Article 25(1) GDPR. However, MPIL failed to implement such measures during the temporal scope.

H. FINDINGS

a) Finding Regarding Article 25(1)

233. The DPC finds that MPIL infringed Article 25(1) GDPR by failing to implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the relevant processing in order to meet the requirements of the GDPR and protect the rights of data subjects.
234. MPIL's failure to implement appropriate measures resulted in a failure to implement the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR. The lack of appropriate measures enabled attackers to use compromised access tokens to gain access to the personal data of Facebook users. The measures applied were not appropriate to implement the principle that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.
235. As set out in detail above, there were a range of additional measures that MPIL could have implemented during the temporal scope to better implement data protection principles and to better address the risk of attackers gaining access to the personal data of Facebook users. While MPIL's non-implementation of any specific measure or group of measures does not in and of itself constitute an infringement of Article 25(1) GDPR, these measures provide context to the consideration of whether the measures

¹⁵⁶ Post-mortem Incident Report, 10.

implemented by MPIL were appropriate at the relevant time under consideration, and as to whether, taking into account the state of the art, the cost of implementation, the particular risks, MPIL, both at the time of the determination of the means for processing and at the time of the processing itself, implemented appropriate technical and organisational measures.

236. The additional measures that MPIL could have implemented include:

- a) Alternative measures to permit users to resume video uploads in the event of disruption or disconnection, which are designed to prevent unnecessary attack vector, and which contain safeguards to ensure the confidentiality of the personal data.
- b) Measures to address the mislabelling of the Facebook for Android access token, which the DPC considers negatively impacted the effectiveness of monitoring and logging measures;
- c) Regular risk reviews and security assessments in order to verify the effectiveness of the chosen measures and safeguards during the temporal scope;
- d) A more appropriate measure than the Facebook for Android access token generated by the Video Uploader feature during the temporal scope; and
- e) A secure coding framework in respect of the access token; internal policies on the secure use of the access token across the Facebook service; and training on the implementation of the access token which meet the principles of data protection by design and by default.

237. The DPC considers that the technical and organisational measures implemented by MPIL during the Temporal Scope were not sufficient to appropriately implement the data protection principles as required by Article 25(1) GDPR and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects. The DPC considers that MPIL failed to implement appropriate measures in respect of the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR. The measures applied were not appropriate to implement the principle that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.

b) Finding Regarding Article 25(2)

238. The principle of Data Protection by Default, which applies under Article 25(2) GDPR, requires that:

by default, only personal data which are necessary for each specific purpose of the processing are processed

and requires controllers to implement appropriate technical and organisational measures to ensure this. In addition, such measures should not by default make personal data available to an indefinite number of persons without intervention by the user.

239. The DPC finds that MPIL infringed Article 25(2) by failing to implement appropriate technical and organisational measures with regard to the scoping and configuration of the access token generated by the Video Uploader feature, to ensure that by default, only personal data which were necessary for its specific purpose were processed. The purpose of the access token was to permit users to resume video uploads in the event of disruption or disconnection. However, despite this purpose, the access token carried full permissions to access all user data available through the Graph API, as well as being able to generate a session cookie for the user. Furthermore, the token was non-expiring.
240. The extent of this access to data was unnecessary for its purpose to resume video uploads in the event of disconnection. As a result of the access token being fully-permissioned, it provided access to a range of personal data regarding Facebook users' accounts. It should instead have had access by default only to the minimum amount of personal data necessary to achieve its purpose, and effectively protect the rights and freedoms of its users. This meant that the access token caused processing of personal data which were not necessary for its purpose. In turn, this resulted in various categories of personal data being affected by the personal data breach.
241. As set out in detail above, MPIL could have implemented appropriate measures to ensure that only personal data which were necessary for each specific purpose of the processing were processed. In particular, MPIL could have limited the permissions associated with the access token, in line with the purpose for which the token was created. The token's access could have been limited so as to not include full access to all the user's profile personal data available from the Graph API. The token could have been limited so as to not include functionality to generate a session cookie from the Graph API. Furthermore, the token did not need to be non-expiring. Accordingly, the DPC finds that MPIL infringed Article 25(2) GDPR through failing to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed.

I. DECISIONS

a) Decision on Corrective Powers in Accordance with section 111(2) of the 2018 Act

242. As set out above, pursuant to section 111(1)(a) of the 2018 Act, the DPC finds that MPIL has infringed Article 25 (1) and Article 25 (2) GDPR.
243. 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 as set out in Article 58(2) GDPR should be exercised in respect of the controller or processor concerned, and, if so, the corrective power to be exercised. The

remaining question for determination in this Decision is whether or not any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and, if so, which corrective powers.

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

[E]ach measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned.

245. Having carefully considered the infringements identified in this Decision, the DPC has decided to exercise certain corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) GDPR. Set out below are the corrective powers that the DPC considers appropriate to address the infringements in the particular circumstances.

246. It is relevant to note that pursuant to Article 58(2)(i) and Article 83(2) GDPR, the DPC has the power, depending on the circumstances of each individual case, to impose an administrative fine in addition to, or instead of, other measures referred to in Article 58(2), as outlined in Recital 148.

247. The DPC has decided to impose the following corrective powers in respect of the infringements identified in this Decision:

- (a) a reprimand to MPIL pursuant to Article 58(2)(b) GDPR; and
- (b) two administrative fines, as follows:
 - i. In respect of MPIL's infringement of Article 25(1) GDPR, a fine of €130 million.
 - ii. In respect of MPIL's infringement of Article 25(2) GDPR, a fine of €110 million.

248. The reasons why the DPC has decided to exercise these corrective powers are set out in further detail below. As noted above, the DPC provided a copy of the PDD to MPIL to afford MPIL the opportunity to provide any further submissions in respect of the provisional findings and the proposed corrective powers. In deciding to exercise corrective powers as set out in paragraph 246, the DPC has also had regard to its power in Article 58(2)(d) GDPR to order the controller or processor to bring processing operations into compliance. However, considering the technical and organisational measures implemented by MPIL since the temporal scope, the DPC does not consider that exercising this power is appropriate, necessary or proportionate in the circumstances.

b) Decision Relating to a Reprimand to MPIL Pursuant to Article 58(2)(b) GDPR

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

250. In terms of the approach that the DPC must take when implementing this power, Recital 129 states:

The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular, each measure must be necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case....

251. MPIL submitted in response to the PDD that a reprimand was ‘not necessary’ to dissuade non-compliance with the GDPR, and likewise that it was not appropriate to the nature of the infringements in question.¹⁵⁷

252. The DPC does not accept that submission and has decided to impose a reprimand on MPIL for the infringements identified in this Decision. The purpose of this reprimand is to dissuade non-compliance with the GDPR. The infringements concern the personal data of nearly 3 million data subjects in the EU/EEA and contributed to a higher risk of fraud, phishing attacks and spamming in respect of affected data subjects. A reprimand is appropriate, necessary and proportionate in respect of such non-compliance in order to fully recognise the serious nature of the infringements and to dissuade such non-compliance. The reprimand will contribute to ensuring that MPIL and other controllers and processors take appropriate steps in relation to current and future operations in order to comply with their obligations regarding data protection by design and by default.

c) Decision Relating to Administrative Fines under Article 58(2)(i) AND 83 GDPR

253. In addition to the DPC’s decision to impose a reprimand under Article 58(2)(b) GDPR, the DPC also considers that the infringements by MPIL of Articles 25(1) and (2) GDPR identified above each warrant the imposition of an administrative fine respectively.

254. 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.

¹⁵⁷ MPIL Submissions on PDD, para 10.2 (Footnote. 132).

255. 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).

256. 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.

257. 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.

258. 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 identified in this Decision respectively.

259. In applying the Article 83(2)(a) to (k) factors to the infringements, the DPC has set 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 infringements of Article 25(1) and the infringement of Article 25(2) 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 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.

d) ARTICLE 83(2) GDPR

- i. **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;**

260. In considering the nature, gravity and duration of MPIL's infringements, the DPC has had regard to the analysis in this Decision concerning the nature, scope, context and purposes of the processing. Article 83(2)(a) requires that the DPC take these matters into account in having regard to the nature, gravity and duration of the infringements. Article 83(2)(a) also requires the DPC to take into account the number of data subjects affected by the infringements and the level of any damage suffered by them.
261. Regarding the **nature of the processing**, the DPC notes that the characteristics of the processing in general relate to personal data shared or otherwise communicated in the context of social media activities. The DPC has set out above that the processing was expansive in nature. The DPC also notes in particular MPIL's own submissions to the effect that the Facebook service runs on a large and complex codebase encompassing multiple millions of lines of code that is constantly evolving. Given the expansive and complex nature of the processing, the DPC considers that it is more difficult for data subjects to fully understand the extent of the risks that may be posed to the various types of personal data processed in the context of their social media activities via the Facebook service.
262. In such circumstances, the DPC considers that users of the Facebook service in general had a greater reliance on MPIL to ensure that their personal data would be appropriately protected. This is particularly so where, as MPIL have confirmed,¹⁵⁸ the users of the

¹⁵⁸ MPIL Response to Sixth Round Queries (Article 33 Inquiry), 3.

services whose personal data were affected by the Breach included children. In light of the foregoing, the DPC attaches significant weight to the nature of the processing.

263. Regarding the **scope of the processing**, the DPC notes that the personal data affected by the Breach were extensive. The scope of the processing relates to the Facebook service, which has 2.32 billion monthly active users globally as of December 31 2018.¹⁵⁹ Any user of the Facebook service was able to interact with the three affected product features and so this figure represents the total number of data subjects who could potentially interact with the three impacted product features and trigger the generation of the Access Token.
264. Further, the manner in which the access token was configured meant that the Video Uploader feature, when triggered to appear in View As mode, had access to any information relating to that user stored on the Graph API.
265. For that reason, the DPC considers that the scope of the processing was extensive both in terms of the number of users of the Facebook service generally, as well as the number of data records potentially impacted by the Breach. Where the scope of processing is extensive it becomes more difficult for data subjects and supervisory authorities to curb unlawful conduct.
266. Regarding the **purpose of the processing**, the DPC notes that this relates to, on the one hand, the ability of users to view and inspect their own personal Facebook page from the perspective of another user via the 'View As' feature and, on the other hand, the ability of users to share video content in the context of sending birthday wishes to other users via the 'Happy Birthday Composer' and Video Uploader features. In this respect, the DPC notes that the purpose of the processing is closely related to the provision, personalisation and improvement (in the sense of the improvement of the user experience) of the Facebook product; which purpose is explicitly specified in the Record of Processing provided by MPIL.¹⁶⁰
267. MPIL submitted in response to the PDD that 'the processing concerned' should be viewed narrowly as simply 'the uploading of videos' rather than the full range of personal data processing operations that were exposed to unauthorised use by means of the Vulnerability as a result of the Breach.¹⁶¹
268. The DPC cannot accept that submission. To adopt such a narrow view of 'the processing concerned' would prevent a comprehensive analysis of the nature and gravity of the infringements. In the circumstances, the processing concerned clearly relates to personal data shared or otherwise communicated in the context of social media

¹⁵⁹ Press Release, 'Facebook Reports Fourth Quarter and Full Year 2018 Results' (30 January 2019), available at: <https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx>.

¹⁶⁰ MPIL Record of Processing, 1.

¹⁶¹ MPIL Submissions on PDD, paras 13.12-15.

activities. The processing exploited in the Breach allowed unauthorised access to wide ranges of Facebook users' personal profile data, and exposed access through Facebook APIs to third-party applications. 'The processing concerned' must therefore be understood as the full range of processing activities relevant to the infringements. In the particular circumstances of the infringements identified in this Decision, the processing concerned is broad and includes processing generally in the context of the social media activities identified.

269. In light of the foregoing, the DPC considers that the purpose of the processing falls within the core activities of MPIL and that the infringements it has identified therefore represent irregularities to which a higher level of severity than normal should be ascribed. In this respect, the DPC considers it appropriate to attribute some weight to this aspect of the processing.
270. Article 83(2)(a) also requires the DPC to take into account the number of data subjects affected by the infringements and the level of damage suffered by them. Therefore, the DPC will first consider these issues before proceeding to consider the nature, gravity and duration of the infringements.
271. Regarding the **number of data subjects** affected as a result of the infringements, the DPC notes that a total of 2 983 092 data subjects were confirmed to have been affected within the EU/EEA. Based on this, the DPC considers the number of data subjects affected is extensive and attributes significant weight to this aspect of the processing.
272. Regarding the **level of damage** suffered by affected data subjects, the DPC considers that the Breach resulted in a loss of control of personal data by the users affected which is a form of 'physical, material or non-material damage' as expressly recognised by Recital 85 GDPR. The Breach could have also resulted in additional physical, material or non-material damage for EU/EEA users, due to the extensive and wide ranging categories of personal data affected by the Breach.
273. The DPC has further considered above the risk of fraud occurring to affected users as a result of phishing attacks (including spear phishing attacks) and spam. The DPC considers that the Breach is likely to have resulted in upset and distress to affected users (also a form of 'physical, material or non-material damage' as expressly recognised by Recital 85) as a result of professional spam and phishing attacks, as well as spear-phishing attacks,¹⁶² which would have been significantly aided by the specificity of data categories affected by the breach.
274. MPIL submitted that even if 'damage' in this context can be taken to include risk, 'the relevant risk is risk stemming from the Video Uploader Token' rather than those arising

¹⁶² [Phishing/Spear phishing — ENISA \(europa.eu\)](#)

from the Vulnerability or the Breach.¹⁶³ For the reasons outlined in paragraph 268, the DPC does not accept this argument.

275. The DPC also does not accept MPIL's assertion that the considerable risks to data subjects identified by the DPC in this Decision are 'speculative and hypothetical' and so not relevant to assessment under Article 83(2)(a).¹⁶⁴ The ability of unauthorised persons to use over-permissioned access tokens to gain unauthorised access to a wide range of Facebook users' personal data as if they were those users themselves, and potentially to third-party applications by the use of those tokens, posed clear and substantial risks that could have had far-reaching consequences. This loss of control is neither speculative nor hypothetical.
276. For the same reasons, the DPC also rejects MPIL's suggestion that 'the only real risk stemming from the Breach is that the email addresses and phone numbers obtained could be used to send unsolicited communications to users.'¹⁶⁵ While those risks featured among those posed by the Breach, the nature of the Vulnerability that allowed the Breach to occur exposed considerably wider ranges of personal data to unauthorised processing, including access, alteration and misuse.
277. Finally, although the DPC acknowledges that MPIL has stated that financial data were not directly affected by the Breach, the DPC has already set out above that certain types of high-risk personal data meriting specific protection and special category data were impacted by the Breach.
278. Taking all of the above into account, the DPC considers that a medium level of damage was suffered or likely to have been suffered by affected data subjects. The DPC accordingly attributes a moderate weight to this aspect of the processing.

Nature of the Infringements

279. The nature of MPIL's infringement of Article 25(1) concerns its failure to implement appropriate measures designed to implement the data protection principles, specifically the principle of integrity and confidentiality in Article 5(1)(f) GDPR, in an effective manner and to integrate the necessary safeguards.
280. The nature of MPIL's infringement of Article 25(2) concerns its failure to ensure, using appropriate technical and organisational measures, that its processing of personal data was, by default, limited to what was necessary in relation to the purposes of that processing and the failure to ensure that only personal data which was necessary for the purposes of the processing was accessible by the access token via the Graph API.

¹⁶³ MPIL Submissions on PDD, paras 13.18-19.

¹⁶⁴ MPIL Submissions on PDD, para 13.21.

¹⁶⁵ MPIL Submissions on PDD, para 13.22.

281. The DPC notes that an infringement of Article 25 GDPR is listed among the infringements of Article 83(4) GDPR and therefore falls within the lower tier of administrative fines under Article 83 GDPR.
282. The DPC is satisfied that the context of the processing in this case (relating to the design of the features to secure the personal data against unauthorised processing and ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed) is central to the aims of Article 25 GDPR. The nature of the infringement is of significance considering the need to prevent unauthorised and unnecessary processing. In light of the risks arising from these infringements, the DPC considers the nature of the infringements of Articles 25(1) and (2) GDPR in this matter to be of medium seriousness.

Gravity of the Infringements

283. On 3 October 2017 the Article 29 Working Party adopted 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679' (the '**Administrative Fines Guidelines**').¹⁶⁶ The Administrative Fines Guidelines were adopted '[i]n order to achieve a consistent approach to the imposition of the administrative fines'.¹⁶⁷ The Administrative Fines Guidelines were endorsed by the EDPB at its first plenary meeting on 25 May 2018.¹⁶⁸
284. The Administrative Fines Guidelines refer to the wording of Article 83(2)(a) in noting that:
- [t]he nature of the infringement, but also 'the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them', will be indicative of the gravity of the infringement.
285. The 'nature... of the processing' (as distinct from the nature of the infringement) is also explicitly referred to in Article 83(2)(a). Interpreted in light of the above-mentioned passage of the Administrative Fines Guidelines, it seems appropriate to consider that this too will be indicative of the gravity of the infringement.
286. In the Breach, the bad actors were provided with unauthorised access to personal data of the impacted data subjects. The submissions from MPIL note its understanding that there were scripted attacks by unauthorised third parties to exploit the vulnerability and collect tokens. It appears likely that the bad actors used those tokens to gain access to the personal data of the associated data subjects. Any personal data actually disclosed

¹⁶⁶ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253, ('**Administrative Fines Guidelines**'), (3 October 2017) available at: <https://ec.europa.eu/newsroom/article29/redirection/document/80836>

¹⁶⁷ Administrative Fines Guidelines, 4.

¹⁶⁸ EDPB Endorsement of Working Party 29 Guidelines, Endorsement 1/2018, (25 May 2018), available at: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

cannot be retrieved or tracked in these circumstances as the controller has lost control of that data. Further processing of the data already collected by the bad actors (before full mitigation was applied by MPIL) and processing by other unauthorised third parties cannot be prevented or tracked.

287. In light of its assessment above as to the nature, scope and purpose of the processing as well as the numbers of data subjects and level of damage suffered by them, the DPC considers that the gravity of the infringements of Article 25(1) and (2) to be of medium seriousness.

Duration of the Infringements

288. The vulnerability that gave rise to the Breach came into existence upon the update carried out to the Video Uploader feature in July 2017. MPIL explained that Meta ‘pushed out the patch for the Vulnerability, at approximately 3:00 a.m. on 28 September 2018’, the result of which ‘was to prevent the attackers from acquiring any additional access tokens through the Vulnerability, thereby fully containing the Attack.’¹⁶⁹ As set out above, the temporal scope of the Inquiry began on 25 May 2018 upon the GDPR coming into force. The lack of appropriate measures related to the entirety of this temporal scope.
289. Accordingly, the DPC considers that the infringements of Articles 25(1) and (2) GDPR lasted from 25 May 2018 to 28 September 2018; a period of just over four months.
290. Taking into account the nature and gravity of the infringements as assessed above, and in particular the nature and scope of the processing as well as the number of data subjects affected, the DPC considers this four month duration of the infringements to be of medium seriousness.

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

291. In assessing the character of the infringements, the DPC notes that the GDPR does not identify the factors that need to be present in order for an infringement to be categorised as ‘intentional’ or ‘negligent’.
292. According to the Administrative Fine Guidelines:

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.¹⁷⁰

¹⁶⁹ Response to First Queries, 7.

¹⁷⁰ Administrative Fines Guidelines, 11.

293. The Administrative Fine Guidelines proceed to detail how supervisory authorities should determine whether wilfulness or negligence is present in a particular case:

The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.¹⁷¹

294. In determining whether an infringement was intentional, the DPC must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration.
295. In determining whether an infringement was negligent, the DPC must determine whether, despite there being no knowledge and wilfulness in respect of the characteristics of the infringement, the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration. As further noted in the Administrative Fine Guidelines:

[C]ircumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence.¹⁷²

296. MPIL's infringement of Article 25(1) GDPR concerns its failure to implement appropriate measures to implement the integrity and confidentiality principle in an effective manner and to integrate the necessary safeguards into the processing. In order to classify these infringements as intentional, the DPC must be satisfied that MPIL (i) wilfully omitted to implement appropriate technical and organisational measures and (ii) knew at the time that the measures that it implemented were not sufficient to meet the standards required by Article 25(1).
297. Having considered the objective elements of MPIL's conduct, the DPC finds that this infringement was of a negligent rather than an intentional character. MPIL negligently allowed the access token to continue to be generated by the Video Uploader feature during the temporal scope despite Meta being aware (and MPIL ought to have been aware) from the time of the ProdSec team's review of the bug bounty report in December 2017 until the Breach occurred in September 2018 that there were certain risks associated with the access token (which is noted above). Those risks were namely, that the FB4A AppID associated with the access token was overly-permissioned in that it provided 'full access to the data in a user's account';¹⁷³ that the access token should

¹⁷¹ Administrative Fines Guidelines, 12.

¹⁷² Administrative Fines Guidelines, 12.

¹⁷³ MPIL submissions on the Inquiry Report, 19.

not have been used by the Video Uploader in a live environment beyond testing;¹⁷⁴ and that it presented an attack surface that could be exploited if the access token were to be exposed to unauthorised parties.

298. Although MPIL ought to have been aware of these risks, it appears that it failed to appreciate the full extent of these risks (and in this respect the DPC notes again the fact that no risk assessment was carried out into the use of the access token with the Video Uploader to support MPIL's assertion that the risk which transpired was unforeseeable). In particular, the DPC notes that ProdSec considered that the risk of the fully-permissioned nature of the access token 'did not create an account takeover vulnerability by itself'¹⁷⁵ (and instead considered that it could be used to allow an attacker to continue controlling an already-compromised account 'even if the original means of access were terminated.')¹⁷⁶ On that basis, the DPC does not consider that MPIL knew at the time that its use and implementation of the access token was not sufficient to meet the standards required by Article 25(1). However, the DPC considers that, given the risks identified following ProdSec's review of the bug bounty report, MPIL ought to have been aware of the inherent risks associated with processing which relies upon the generation of an access token (which serves an authentication/authorisation function), and that wherever there is any token generated by a piece of code, there is a risk that it will be misused by unauthorised parties. In light of the foregoing, the DPC considers MPIL's infringement of Article 25(1) to be negligent. In light of the level of negligence, this is an aggravating factor of moderate weight in the circumstances.
299. The DPC rejects MPIL's submission that the DPC's approach amounts to treating the mere fact of an infringement as an aggravating factor.¹⁷⁷ MPIL's use of the over-permissioned access token was not simply a choice that had unforeseeable results allowing the Breach to occur. The risks were foreseeable and identified at least from 7 December 2017, and MPIL did not properly assess and mitigate them while it had an opportunity to do so. Use by a controller of an insecure or otherwise inappropriate means of processing can occur for multiple reasons. MPIL's failure to assess and mitigate the risks posed by its means of processing resulted on a significant level of negligence, which is the factor that aggravates the infringement in this case.
300. Turning to Article 25(2) GDPR, MPIL's infringement of Article 25(2) concerns its failure to ensure, using appropriate technical and organisational measures, that its processing of personal data was limited to what was necessary in relation to the purposes of the processing. In order to classify this infringement as intentional, the DPC must be satisfied that MPIL (i) wilfully allowed for the use by the Video Uploader of the fully-permissioned

¹⁷⁴ As noted above at paragraph 133, 'the engineer tasked with writing the code to generate the access token made it clear that its use was inappropriate and should not be launched to the public.'

¹⁷⁵ MPIL submissions on the Inquiry Report, para 5.6.

¹⁷⁶ MPIL submissions on the Inquiry Report, para 5.6.

¹⁷⁷ MPIL Submissions on PDD, paras 13.30-13.34.

access token and (ii) that it knew at the time that this would result in personal data processing that was not limited to what was necessary in relation to the purposes.

301. It is not in dispute that MPIL, as controller, was responsible for the decision to use the access token in the manner set out above. As explained above, the purpose of the access token was to permit the user to resume video uploads via the Video Uploader in the event of disruption or break in internet connectivity. Where such a break in connectivity occurred, the access token functioned to provide authentication or proof to the Video Uploader that the user seeking to upload a partially-uploaded video was the same user that began that upload prior to the break in connectivity. As set out above, in accordance with Article 25(2) GDPR and the principle of data minimisation, the access token should not have been fully-permissioned but should instead only have had access by default to the minimum amount of personal data strictly necessary to achieve its purpose, and effectively protect the rights and freedoms of its data subject users.
302. However, the DPC is not satisfied MPIL knew that the access token was not strictly necessary for this purpose, and that it wilfully insisted upon its continued use. On that basis, the DPC does not find this infringement to have been intentional. For instance, and although as noted above, following its review of the bug bounty report 'ProdSec recommended the creation of a new app ID, with narrower permissions to be associated with it, to be used for the Video Uploader',¹⁷⁸ the DPC notes that MPIL believed that the access token 'did not provide the receiving user with any greater privileges than they were supposed to have' and that 'the user of a Facebook account is entitled to have full privileges with respect to the data in their own account.'¹⁷⁹ However, the DPC considers that MPIL erred in this respect, given that the purposes of the processing relate to the Video Uploader rather than the user's entitlements when logged in to their own account. In order for the Video Uploader to function as MPIL intended, it simply required a means of authenticating the user who instigated the video upload prior to any break in connectivity, and therefore did not require access to all of the data available on that user's account. As is evident from ProdSec's review of the bug bounty report as considered above, and recommendations made regarding the use of a more narrowly-permissioned access token and thereafter attempts made to replace or modify the access token, the DPC is satisfied that MPIL ought to have been aware that the fully-permissioned nature of the Access Token was not strictly necessary for the purposes of the Video Uploader.
303. In light of the foregoing, the DPC considers MPIL's infringement of Article 25(2) to be negligent and finds that the level of this negligence is an aggravating factor of moderate weight in the circumstances.

¹⁷⁸ MPIL submissions on the Inquiry Report, 19 - 20.

¹⁷⁹ MPIL submissions on the Inquiry Report, para 14.6.

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

304. As noted in the Administrative Fine Guidelines, organisations should ‘do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned,¹⁸⁰ whilst also acknowledging the existing obligations on such organisations to implement appropriate security measures and to mitigate risks.¹⁸¹ Accordingly, for an action or measure to be considered mitigating for the purposes of Article 83(2)(c), that action or measure must be distinct from and additional to those which are already required to be taken.

Incident Response

305. As noted above, MPIL’s formal incident response procedures were engaged on 25 September 2018. Details of what these procedures entailed were set out as part of the Incident Report¹⁸² and consisted of the patching of the vulnerability, the containment of the attack and additional follow-up measures including the revision of the Video Uploader and View As features, enhancements to various tools relating to account takeover and bug detection, enhancements to logging practices, and certain additional actions.¹⁸³ As noted above, MPIL stated that its remediation plan ‘was fully executed in less than 48 hours, at which time it appears that the conditions of the vulnerability that gave rise to the Breach were fully remediated. Although the DPC has found that there were certain design elements to the access token which likely contributed to a delay in the time taken for MPIL to identify that the attack was occurring (and which therefore likely had a knock-on effect on the time it took before MPIL’s remediation plan could be implemented), the DPC considers this 48-hour timeframe between the rollout of the remediation plan and its execution to be expedient and therefore a mitigating factor.
306. Regarding the actions taken by MPIL prior to the engagement of the incident response procedures, the DPC has had regard in particular to the Expert Report of Professor Siegel. Professor Siegel described MPIL’s response to the Breach as being ‘exceptionally quick’,¹⁸⁴ noting that ‘[i]t took [Meta] 11 days from the commencement of the Attack to determine that an attack was in progress’¹⁸⁵ and compared the response time to those involved in the ‘18 biggest data breaches known at the time’ as published by CSO Online (described as ‘a news website covering cybersecurity for IT security professionals.’)¹⁸⁶ In

¹⁸⁰ Administrative Fines Guidelines, 12.

¹⁸¹ ‘The data controllers and processors have an obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and mitigate risks arising from the processing of personal data to the rights and freedoms of the individuals.’ See Administrative Fines Guidelines, 12.

¹⁸² Incident Report, 6.

¹⁸³ Incident Report, 8-11.

¹⁸⁴ Expert Report, para 41.

¹⁸⁵ Expert Report, para 43.

¹⁸⁶ Expert Report, para 42.

that publication, the average time period from attack to detection across 17 of these breaches was said to be 316 days.¹⁸⁷

307. Although the DPC has carefully considered the points made by Professor Siegel, it must consider the Breach on its own facts. By contrast, the DPC considers that Professor Siegel's report does not consider any of the 18 breaches referred to on their facts but simply considers the response times to the breaches in the aggregate and absent of any relevant context. The DPC further considers the unique position occupied by MPIL to be of relevance here, particularly in terms of the resources available to it and the nature, scope and complexity of its processing activities associated with the Facebook service. As set out above, the DPC considers that there were certain design aspects to the access token that likely contributed to a delay in the time it took MPIL to identify that the attack was occurring and to thereafter formally engage its incident response procedures. The DPC therefore cannot consider the time MPIL took to detect the Breach as a mitigating factor.

Mitigation of Risks to Third Party Applications

308. The DPC also notes the actions taken by MPIL in addressing the potential risks posed by the Breach to third-party applications that allow for authentication of users via their Facebook login details (in which case, where a user's Facebook account had already been compromised, this would also allow for that user's linked third-party account(s) to be compromised.) MPIL explained both in its responses to queries raised in the Inquiry¹⁸⁸ and again in its submissions on the Inquiry Report how, having investigated the matter, it 'was able to determine that Third Party Accounts were not affected' by the Breach.¹⁸⁹ However, MPIL stated '[i]n parallel with investigating whether the attackers accessed Third Party Accounts as part of the Attack, [Meta] developed a remediation plan – discussed in advance with [MPIL] – to ensure the protection of users' Third Party Accounts regardless.'¹⁹⁰
309. Some developers of third-party applications allowed users to login to those applications via the Facebook Login function. As part of the remediation plan, MPIL launched a tool to allow those developers to identify (using 'hashed and encrypted User IDs')¹⁹¹ any of their users who were affected by the Breach and to reset those users' access tokens, thereby requiring them to login again manually to the third-party application.¹⁹² MPIL explained that this tool was intended for use by developers who had built their applications otherwise than through MPIL's own 'Software Development Kit' ('SDK'),

¹⁸⁷ Expert Report, para 44.

¹⁸⁸ Response to First Queries, 8.

¹⁸⁹ MPIL submissions on the Inquiry Report, para 7.12.

¹⁹⁰ Response to First Queries, 9.

¹⁹¹ Response to First Queries, 10.

¹⁹² Response to First Queries, 9-10.

because ‘applications that use the [SDK] implementation of Facebook Login automatically check the validity of a user’s Facebook access token whenever the user accesses the application.’¹⁹³ Accordingly, any access token created for a third-party application that had been built using the SDK would have been invalidated as part of the actions taken by MPIL to invalidate the Access Token starting 27 September 2018.

310. It was important that the Breach was remediated in a timely manner. The DPC has taken this into account and has noted that, once MPIL’s formal remediation plan was put in place, MPIL acted promptly to remediate the conditions of the vulnerability that gave rise to the Breach. The DPC also considers MPIL’s additional timely actions in relation to third-party applications to be of mitigating value.

Security Enhancements

311. In addition to the ‘immediate technical remediation’¹⁹⁴ actions to patch the vulnerability, invalidate the access token, disable the View As feature and revise the Video Uploader,¹⁹⁵ MPIL and Meta ‘undertook a longer-term effort to study the lessons from the Attack in order to identify any other ways to strengthen relevant measures against the risk of any similar incident occurring in the future.’¹⁹⁶ A number of security enhancements were made on foot of this, which were set out in more detail in MPIL’s Response to Fourth Queries¹⁹⁷ and its Response to Fourth Queries Update,¹⁹⁸ and which were summarised by MPIL in its submissions on the Inquiry Report,¹⁹⁹ all of which the DPC has carefully considered.²⁰⁰
312. Although the DPC does not consider that these security enhancements had any impact on mitigating the damages or risks caused by the Breach itself, it does consider that they were specifically targeted at addressing the types of risks that were directly relevant to the Breach. On that basis, the DPC considers these enhancements to be demonstrative of MPIL’s (and Meta’s) capacity to prevent future occurrences of breaches of a similar nature.

¹⁹³ Response to First Queries, 9.

¹⁹⁴ MPIL submissions on the Inquiry Report, 23.

¹⁹⁵ As described in both Incident Report at 8-9 and MPIL submissions on the Inquiry Report, 23-24.

¹⁹⁶ MPIL submissions on the Inquiry Report, para 9.2.

¹⁹⁷ Response to Fourth Queries, 3-5.

¹⁹⁸ Response to Fourth Queries Update and Exhibit 1 - Summary Security Improvements (Exhibit 1 - Summary Security Improvements consists of a summary provided by Meta to MPIL of the additional work which had been done since the Incident Report).

¹⁹⁹ MPIL submissions on the Inquiry Report, para 9.3.

²⁰⁰ The Incident Report also noted as part of its list of ‘Additional Follow-Up Measures’ the consolidation and expansion of ‘security documentation for software engineers with regard to the secure use of access tokens’ – see Incident Report, 10. However, as set above in this Decision, although such documentation was stated to have been ‘published on Facebook’s internal wiki’, copies of same were not provided to the DPC in the course of the Inquiry.

313. For example, MPIL detailed in its submissions on the Inquiry Report its enhancements to 'various defence-in-depth controls against access token abuse and expanding existing compromise detection tools and logging systems so as to facilitate detection and investigation of any future incident involving large-scale access token theft.'²⁰¹ These enhancements included a new 'Login Service' [REDACTED] [REDACTED] the introduction of a means of limiting the permissions associated with certain first-party access token permissions; improvements to the 'Sentry' framework [REDACTED] where a vulnerability is suspected; enhancements to the Growth Team's alerting tools; [REDACTED] [REDACTED] and updates to metadata associated with access tokens to better determine whether they may have been generated as a result of suspicious activity.²⁰²
314. The DPC considers that, in principle, the improvements identified above all represented reasonable approaches to be taken to some of the security issues that arose. For that reason, the DPC considers that these improvements are demonstrative of a reasonable, forward-thinking approach on the part of MPIL designed to mitigate the risks posed by any future occurrence of a breach of a similar nature to the Breach at issue in this Inquiry. The DPC therefore considers these improvements to be of mitigating value.
315. In addition to the security enhancements referred to above, MPIL instructed an Expert Measures Review be carried out by a third party into its technical and organisational security measures. MPIL provided an overview of a number of improvements made to MPIL's incident management and oversight measures following the completion of the Expert Measures Review, which are set out in the Response to Fourth Queries²⁰³ and Response to Forth Queries Update²⁰⁴ and are summarised by MPIL in its submissions on the Inquiry Report. The DPC considers the fact that MPIL arranged for the Expert Review to be undertaken is demonstrative of positive efforts on the part of MPIL to reassess and make changes to its technical and organisational measures in order to improve its oversight of Meta's processing activities and to improve both Meta's and its own incident management capabilities.
316. However, the improvements made on foot of the Expert Measures Review relate to the Facebook service more generally (as opposed to the specific enhancements related to access tokens considered above) and as such the DPC does not consider that these actions were likely to have had a mitigating impact on 'the damage suffered by data subjects', as is required pursuant to the wording of Article 83(2)(d). In those

²⁰¹ MPIL submissions on the Inquiry Report, para 9.3.

²⁰² MPIL submissions on the Inquiry Report, para 9.3.

²⁰³ Response to Fourth Queries, 4.

²⁰⁴ Response to Fourth Queries Update.

circumstances, the DPC does not consider the improvements made on foot of the measures review to be of mitigating value.

317. Overall, the DPC considers that the various actions taken by MPIL identified in this section were of moderate mitigating value and has taken this into account in its determination as to the fine to be imposed.

iv. 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

318. The Administrative Fine Guidelines refer to the existing obligations imposed on controllers under Articles 25 and 32 GDPR and state that:

[t]he question that the supervisory authority must then answer is to what extent the controller 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.²⁰⁵

319. The DPC has found that MPIL infringed Articles 25(1) and 25(2) regarding its processing of personal data. The DPC considers that MPIL holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. It is clear that MPIL did not do 'what it could be expected to do' in the circumstances assessed in this Decision. However, in circumstances where this factor forms the basis for the finding of the infringements of Article 25 against the MPIL, this factor cannot be considered aggravating in respect of the infringements. Rather, the DPC must independently consider pursuant to Article 83 whether these infringements of Article 25 merit the imposition of administrative fines in and of themselves.

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

320. No relevant previous infringements arise for consideration in this context. This therefore constitutes a neutral factor in the circumstances.

vi. 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;

321. While the DPC acknowledges MPIL's cooperation in the course of the Inquiry, MPIL was under an existing obligation to do so pursuant to Article 31 GDPR and the DPC does not consider that these actions went above or beyond what was already required of MPIL pursuant to Article 31 GDPR.
322. In light of the foregoing, the DPC considers MPIL's degree of cooperation with the DPC to be a neutral factor.

²⁰⁵ Administrative Fines Guidelines, 12.

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

323. The affected personal data relates to social media content, which is typically personal to the user who posts the information, including a wide range of information about a person's life.
324. As noted above, the categories of personal data affected by the infringement are set out in the Appendix to this Decision and included personal data such as a user's full name, email address, phone number, location, place of work, date of birth, religion, gender, posts on timelines, groups of which a user was a member, and certain message content.
325. In its submissions on the PDD, MPIL observes correctly that Article 83(2)(g) requires account to be taken of the categories of personal data affected by 'the infringement' rather than 'the Breach', as referred to in the PDD.²⁰⁶ The DPC considers that the over-permissioned access token that permitted the Breach to occur exposed an extensive range of personal data to unauthorised access. That wider range of personal data is therefore the proper subject of consideration in this regard.
326. As set out above, the DPC considers that categories of data affected by the infringements also included special categories of personal data and children's personal data. In this respect, the DPC has noted above that MPIL confirmed that children's personal data was affected and that MPIL confirmed that data revealing religious beliefs were affected (the latter constituting special category data pursuant to Article 9(1) GDPR).
327. In addition, as explained above, the DPC considers that special category data in the form of data concerning sexual orientation were affected. The DPC has further considered above that data concerning a person's sex life were also affected in light of MPIL's confirmation that data revealing both gender and relationship status were impacted. In this regard, the DPC considers that 'data concerning a natural person's sex life is to be broadly construed'²⁰⁷ and that, where a user also specifies their relationship status,²⁰⁸ these data constitute special category data for the purposes of Article 9(1) GDPR.
328. The DPC is accordingly satisfied that data concerning a natural person's sex life and data concerning a natural person's sexual orientation were both impacted and that, in addition to data revealing religious beliefs, such data represent a further type of special category data to have been affected by the Breach.
329. Regarding the risks associated with the categories of data affected impacted, the DPC considers that, by their nature, these categories of personal data carry a risk with regard

²⁰⁶ MPIL Submissions on PDD, para 13.5.

²⁰⁷ Christopher Kuner, Lee V. Bygrave & Christopher Docksey, *"The EU GDPR: A Commentary"* (Oxford, 2020), 375.

²⁰⁸ As noted at footnote 207 above, Kuner et al. give express consideration to marital status and how details on a person's marital status come within the meaning of Article 9(1) GDPR. This also aligns with the views expressed by the CJEU in Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601, paras 122-127.

to the fundamental rights and freedoms of data subjects. The DPC notes that MPIL argued in its submissions on the Inquiry Report that [t]he types of data exposed do not include types of data that are well suited for identity theft or fraud, pointing to its position that no financial data or passport or national ID numbers were affected by the Breach and that, '[w]ithout such information, an attacker cannot open financial accounts or make purchases using someone else's identity.'²⁰⁹ On the contrary, the DPC is satisfied that certain other information impacted in the Breach, in particular, phone numbers and email addresses, can be targeted for fraud, impersonation and spamming.

330. Phone numbers and email addresses are persistent forms of personal data, which are infrequently changed or abandoned by the holder. These contact details are frequently used as personal identifiers in the context of numerous online and offline services, posing a potential fraud risk where these personal data are utilised. The DPC further consider that the types of risks associated with fraud are not limited to financial risks, as MPIL appears to suggest in its submissions on the Inquiry Report.²¹⁰ Where phone numbers and email addresses can be linked to other personal data, such as a user's full name, the risk of fraud and impersonation increases significantly and users are placed at a heightened risk of being the victims of serious forms of fraud, including financial fraud, impersonation and loss, whether that be financial, of their personal data and/or of private and confidential information more generally.
331. There is an overlapping risk of data subjects being potentially directly affected by the disclosure of their personal data and those who know such persons being subjected to a range of scams. The risk of phishing and spear phishing scams has been considered above, whereby fraudsters leverage email addresses in order to trick persons into disclosing or inputting confidential passwords or codes, or where fraudsters may impersonate a data subject who has had their personal data disclosed in order to defraud others. Other scams may include 'smishing' scams, whereby fraudsters leverage phone numbers in the same manner. The potential severity of consequences to individuals is plainly quite high, given both the categories and the range of personal data that have been disclosed.
332. It is noteworthy that MPIL itself stated in the updated breach notification form its belief that 'the main impact for affected users will be an increased likelihood that they will be the target for professional 'spam' operations' and also noted that '[t]here may also be an increased risk of individuals being the target for "phishing" attacks.'²¹¹ Although MPIL asserted that the level of risk was low, the DPC has considered above the significant risks that can result from such attacks and spam operations, including potentially major financial loss (though the DPC notes again that MPIL has stated that financial data were not directly impacted by the Breach), distress to users, and the installation of viruses and

²⁰⁹ MPIL submissions on the Inquiry Report, para 19.6(c)(1).

²¹⁰ *ibid.*

²¹¹ Updated Cross-Border Breach Notification Form, 17.

other malware which can cause serious interference and interruption to users' computer systems.

333. The risk posed by the disclosure of phone numbers in particular is particularly high. In addition to the risk of smishing scams outlined above, fraudsters can also use phone numbers to engage in extensive fraud and impersonation through 'SIM-swapping', whereby mobile carriers are tricked into transferring a data subject's phone number to a fraudster's device in order to carry out fraudulent activities, such as gaining access to bank accounts or resetting email and social media account credentials.
334. In addition, the DPC notes that the data subjects affected may include children and vulnerable people. It is not practicable for the purposes of this Inquiry to analyse the specific personal data actually shared by children on their Facebook accounts (or on other services accessible through the common Access Token). Such services allow users to share their personal data through messages, audio, video calls and video chats, and by sending images and video files, including through public comments and conversations. Data subjects interact with the Facebook service on foot of an understanding that certain aspects of their social media content would be visible only to restricted sets of people, such as Friends of Friends of Friends. Other personal data may be stored within the account that is not intended to be shared with any other person. Data subjects were not informed that such content was subject to access by an indefinite and unrestricted audience through the inadvertent provision of full access tokens. In all the circumstances, I am satisfied that the categories of personal data likely stored by data subjects, including children and vulnerable adults, on their accounts include an extensive range of categories. This personal data shared is likely to include information on users' daily lives and interests. The personal data may be sensitive as it may make a child user identifiable to dangerous persons due to the unauthorised processing of that personal data.
335. In light of the foregoing analysis, the DPC considers that the categories of personal data affected were significant both in terms of the amount of data impacted regarding each data subject and in terms of the types of risks posed. The DPC also considers that the types of risks posed were further compounded where special category data and children's data were impacted.
336. Taking all of the above into account, the DPC considers that the categories of personal data affected by the Breach are of high seriousness. This is significantly aggravating in the circumstances.

- viii. **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;**
337. The infringements identified became known to the DPC by way of a breach notification submitted pursuant to Article 33(1) GDPR. According to the Administrative Fine Guidelines:
- [T]he controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor.²¹²
338. On that basis the DPC considers this factor to be neutral.
- ix. **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;**
339. According to the Administrative Fine Guidelines, ‘this assessment criterion only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors “with regard to the same subject matter.”’²¹³
340. No such measures have previously been ordered against MPIL and the DPC accordingly considers this to be a neutral factor.
- x. **Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;**
341. No such considerations arise in this matter.
- xi. **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;**
342. The DPC notes that it has commended MPIL in relation to how it provided prompt and effective remediation of the token breach.²¹⁴ Further, DPC considers that MPIL’s steps taken after the Breach to improve documentation and training should be considered as a mitigating factor.²¹⁵
343. The DPC is satisfied that the matters set out above and under Articles 83(2)(a) to (k) give a full account of the factors to which it should have due regard in the context of Article 83(2) GDPR.

²¹² Administrative Fines Guidelines, 15.

²¹³ *ibid.*

²¹⁴ See para 161.

²¹⁵ See para 231.

J. DECISION AS TO WHETHER TO IMPOSE AN ADMINISTRATIVE FINE AND, OF SO, THE AMOUNT OF THE FINE

344. 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.
345. The DPC has also had regard to the effect of the reprimand in ensuring compliance with the GDPR. The reprimand will contribute towards dissuading future non-compliance by formally recognising the moderate nature of the infringements. However, the DPC considers that the reprimand alone is not sufficient in the circumstances to ensure compliance. The DPC finds that an administrative fine in respect of the infringements is appropriate, necessary and proportionate to ensure compliance with the GDPR.
346. 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.

347. The DPC does not consider the reprimand alone appropriate to deter other future serious infringements. 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 a reprimand alone 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:

- a. As set out in its assessment of Article 83(2)(a), both of the infringements are of medium seriousness in nature, gravity and duration and must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. This is particularly so given the types of damage suffered (which, at a minimum included a loss of control over personal data) or likely to have been suffered (which included upset and distress as a result of professional spam and phishing attacks) by the data subjects as a result of the infringements, and the fact that the infringements affected nearly 3 million data subjects within the EU/EEA.
- b. Regarding the infringement of Article 25(1), in circumstances where MPIL failed to modify the design to reflect concerns raised about the appropriateness of the access token for the particular processing in question, given the nature, gravity and duration of the infringements as set out in the DPC's assessment of Article 83(2)(a) above, the DPC considers that MPIL's non-compliance with its obligations under Article 25(1) must be very strongly dissuaded. This is particularly the case given the nature and categories of the personal data as considered above, and the risks associated with same, which included fraud, impersonation and spamming, phone numbers, email addresses and, in certain cases, location data. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, the DPC considers that an administrative fine is appropriate and necessary in the circumstances.
- c. Regarding MPIL's infringement of Article 25(2), processing of users' personal data in a manner that is not limited to what is necessary in relation to the purposes of that processing must be strongly dissuaded. The use of a fully-permissioned access token presented an additional, unnecessary attack vector which was ultimately exploited in the attack (which also involved the Access Token being exchanged for a session cookie). If MPIL limited the permissions associated with the access token to what was strictly necessary to the required functionality of the Video Uploader, the attack would not have been able to propagate as it did, and significantly less personal data would have been impacted. As a result, MPIL lost control of the personal data and exposed the data subjects to the risks of fraud, spamming and impersonation which the DPC has considered above. Given that the risks of fraud, spamming and impersonation constitute a high risk to the rights and freedoms of natural persons, which could lead to physical, material or non-material damage, the DPC considers that an administrative fine is appropriate and necessary in order to dissuade non-compliance.
- d. Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate in the circumstances in

view of ensuring compliance. The damage suffered (which, at a minimum included a loss of control over personal data) or likely to have been suffered (which included upset and distress as a result of professional spam and phishing attacks) by the data subjects as a result of MPIL's infringements affected nearly 3 million data subjects within the EU/EEA. The DPC considers that the types of damage identified constitute significant damage in the circumstances. In light of this damage, and how it was suffered by a significant number of users, the DPC considers that a fine is proportionate to responding to MPIL's infringements with a view to ensuring future compliance. Again, the nature of the personal data at issue is also relevant here. The DPC considers that a fine does not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

- e. The DPC considers that the negligent character of MPIL's infringement of Article 25(1) carries weight when considering whether to impose an administrative fine, and if so, the amount of that fine. As set out above, MPIL ought to have been aware that its measures were not sufficient in respect of the need to implement the data-protection principles in an effective manner. This negligence suggests that an administrative fine is necessary to effectively ensure that MPIL directs sufficient attention to its obligations under Article 25(1) in the future.
- f. The DPC also considers that the negligent character of MPIL's infringement of Article 25(2) GDPR carries weight when considering whether to impose an administrative fine, and if so, the amount of that fine. As set out above, MPIL ought to have been aware that the fully-permissioned nature of the Access Token was not strictly necessary for the purposes of the Video Uploader. This negligence suggests that an administrative fine is necessary to effectively ensure that MPIL directs sufficient attention to its obligations under Article 25(2) GDPR in the future.
- g. As set out in the DPC's assessment of Article 83(2)(g), the categories of the personal data affected by the infringements were also serious and, as a result of the infringements, meant that data subjects were exposed to the risks of fraud, spamming and impersonation which have been considered above. Given that the risks of fraud, spamming and impersonation could lead to physical, material or non-material damage, the DPC considers that administrative fines are appropriate and necessary in order to dissuade non-compliance. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures.
- h. The DPC considers that administrative fines would help to ensure that MPIL and other similar controllers take the necessary action to ensure the upmost care is taken to avoid infringements of the GDPR in respect of users' data. In these particular circumstances where the categories of user's data affected by MPIL's

infringements carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft and fraud, the DPC considers that administrative fines are appropriate and dissuasive.

- i. The DPC has had regard to the actions taken by MPIL in order to mitigate the damage caused by the Breach and to prevent further recurrences of breaches of a similar nature. As set out above, the DPC considers that these factors were of mitigating value and has taken them into account when calculating the administrative fines. However, despite these factors, the DPC considers that administrative fines are appropriate, necessary and proportionate in respect of each infringement in order to ensure compliance with the GDPR. The DPC considers that the need to dissuade non-compliance of this nature concerning the personal data of millions of data subjects far outweighs the mitigation applied for this factor. The DPC notes that the data subjects affected include children and vulnerable people, as well as special category data in the form of data revealing religious beliefs, data concerning sex life and data concerning sexual orientation. In light of the negligent character of the infringements, and MPIL's failure to comply with its obligations with regard to data protection by design and default, the DPC considers that a dissuasive administrative fine is necessary in the circumstances to ensure future compliance.

348. In its submissions on the PDD, MPIL objected not just to the DPC's proposal to impose administrative fines and the amounts of those fines, but also to the fact that the DPC proposed to issue two separate fines for infringements of Article 25(1) and 25(2) GDPR respectively.²¹⁶ MPIL submitted in that regard:

..the proposed fines are procedurally disproportionate, as they would punish MPIL twice for the same conduct and alleged wrongdoing, which violates fundamental principles of EU and Irish law and would in itself contravene Article 83(1)... the DPC's proposed finding of Article 25(2) infringement concerns the use of a fully permissioned access token in connection with the Video Uploader – which is conduct and alleged wrongdoing already covered by the proposed finding of Article 25(1) infringement.²¹⁷

349. In a related submission on the same point, MPIL stated:

The making of these two findings of infringement would not necessarily be problematic were the DPC not to impose separate fines for each alleged infringement. Yet that is what is proposed in the PDD. MPIL respectfully submits that this approach is unlawful and would effectively punish MPIL twice in respect

²¹⁶ MPIL Submissions on PDD, para 12.1-7.

²¹⁷ *ibid*, para 12.1.

of the same alleged wrongdoing, which is inconsistent with Irish and EU law principles.²¹⁸

The DPC has carefully considered MPIL's submissions in this regard and rejects them. The GDPR specifies particular obligations that bear distinct corrective measures. The DPC has detailed distinct conduct that was found to have infringed Article 25(1) and Article 25(2) GDPR. The DPC is entitled to impose separate administrative fines in respect of these distinct violations. As set out above, MPIL's infringement of Article 25(2) related to the scoping and configuration of the access token generated by the Video Uploader feature in that the access token carried full permissions to access all user data available through the Graph API, as well as being able to generate a session cookie for the user. While MPIL's failure to limit the permissions is also relevant to the infringement of Article 25(1) GDPR, the DPC has taken this overlap into account when calculating the fines. The fine imposed for the infringement of Article 25(1) GDPR relates only to the portion of that infringement that does not overlap with the infringement for which the Article 25(2) fine was imposed. In particular the fine for the infringement of Article 25(1) GDPR has not taken into account the fact that the access token carried full permissions, but has instead only taken account of the other factors leading to the infringement of Article 25(1) GDPR as detailed in this Decision.

350. 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 25(1) GDPR, a fine of between €110 million and €150 million, and
 - (b) In respect of MPIL's infringement of Article 25(2) GDPR, a fine of between €75 million and €115 million.
351. 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 25(1) GDPR, a fine of between €110 million and €130 million, and
 - b. In respect of MPIL's infringement of Article 25(2) GDPR, a fine of between €70 million and €110 million.
352. Based on the analysis set out in this Decision, and following its consideration of the views of three Concerned Supervisory Authorities²¹⁹ and the subsequent further submissions of MPIL on those views and on the question of the appropriate fines, the DPC has

²¹⁸ *ibid*, para 9.6.

²¹⁹ Views expressed by the supervisory authorities of Hungary ('HU SA'), France ('FR SA') and Hamburg ('Hamburg SA'). See Part M of this Decision *Selection of Amounts of Administrative Fines*, below.

decided to impose the following administrative fine in respect of MPIL's infringements of Article 25 GDPR:

- (a) In respect of MPIL's infringement of Article 25(1) GDPR regarding the processing, a fine of €130 million.
- (b) In respect of MPIL's infringement of Article 25(2) GDPR regarding the processing, a fine of €110 million.

- 353. In determining 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. The DPC has taken into account – in accordance with the approach of the EDPB as set out in detail below – Meta's turnover as set out below in its calculation of the appropriate amount of the administrative fines. The DPC considers it 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.
- 354. 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 medium seriousness in nature and in gravity. The infringements concern the personal data of Facebook users and the infringements all increased the risks posed by the processing to the right and freedoms of those data subjects, in particular in relation to the risk of fraud, impersonation, and spamming.
- 355. 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.
- 356. As regards the requirement for any fine to be proportionate, this requires the DPC to adjust the quantum of any proposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. The DPC is satisfied that the fines above do not exceed what is necessary to enforce compliance with the GDPR taking into account the size of MPIL's user base, the loss of control over personal data suffered by the data subjects, how infringements increased the risks posed by the processing to the right and freedoms of the data subjects and the mitigating factors identified in this Decision. The DPC has also taken due account of the comments received from CSAs during the Article 60 process.
- 357. The DPC is satisfied that the two fines specified above, if imposed on MPIL, would be effective, proportionate and dissuasive, taking into account all of the circumstances of this Inquiry.

358. In its submissions on the PDD, MPIL argued that the proposed administrative fines were disproportionate to the infringements found by the DPC:

The infringements of Article 25 provisionally found in the PDD relate to the design and use of the Video Uploader Token. The Video Uploader Token was not tantamount to the Vulnerability, nor was it a sufficient cause of the Breach.

[...]

The PDD asserts that MPIL should have foreseen the possibility that the Video Uploader Token could combine with other unknown features in some unknown way that could lead to some kind of data breach like the Breach. As MPIL has explained, however, there was no reason to foresee any such risk at the relevant time. Even to the extent the DPC disagrees, the DPC should acknowledge that the PDD's finding is not that the Video Uploader Token caused the Breach; rather, the PDD's finding is that the Video Uploader Token *contributed to a risk of an unknown vulnerability arising* that in turn might lead to a data breach. Any fine imposed by the DPC must be assessed by reference to this comparatively limited finding of alleged infringement – as opposed to being based on the Breach itself.²²⁰

359. The DPC does not agree with this submission. As has been explained in detail in this Decision, the infringements found in this case relate to risks that could and should have been foreseen and addressed before the attack. The infringements affected a broad range of personal data concerning nearly 3 million Facebook users, and placed them at considerable risk. Based on this and the other reasons stated above, the DPC is satisfied that the administrative fines are proportionate.

K. ARTICLE 83(3) GDPR

360. Having completed its assessment of whether or not to impose a fine (and of the amount of each such fine), the DPC must now consider the remaining provisions of Article 83 GDPR, with a view to ascertaining if there are any factors that might require the adjustment of the fines.
361. 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.

²²⁰ MPIL Submissions on PDD, paras 11.3-11.4.

362. The EDPB adopted a binding decision (**'the EDPB Decision concerning WhatsApp'**) 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.
363. 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 it is a matter of general interpretation that is not specific to the facts of the case in which it arose. 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 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.²²¹
364. The impact of this interpretation is that administrative fine(s) should be imposed cumulatively, as opposed to imposing only the proposed 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 (see below).
365. In this Decision, the DPC has found that MPIL has infringed Articles 25(1) and (2) GDPR. The DPC considers that MPIL’s infringement of Article 25(1) is the gravest infringement. Whilst both infringements are serious, the DPC considers that the effects of the infringement of Article 25(2) primarily related to the amount of personal data that became accessible to the attacker in the course of the attack and that allowed the attack propagate across other accounts as a result of the fully-permissioned default configuration of the access token. On the other hand, the DPC considers that the infringement of Article 25(1) was what allowed the attack to occur in the first place insofar as the design, configuration and operation of the Video Uploader to generate the

²²¹ The EDPB Decision concerning WhatsApp, 64-66.

access token was what created the attack surface exploited in the attack. It is for this reason that the DPC considers the infringement of Article 25(1) to be the graver of the two.

366. Articles 83(4)-(6) do not distinguish between subparagraphs for the purposes of establishing the categories into which an infringement falls. The infringements of both subparagraphs of Article 25 fall to be considered individually, for the purposes of calculating the fine, under Article 83(4) GDPR. Article 83(4) provides, *inter alia*, that an infringement of Article 25(1) or (2) shall be subject to an administrative fine up to €10 000 000, or in the case of an undertaking, up to 2% of the total worldwide turnover of the preceding financial year, whichever is higher. As such, in accordance with Article 83(3), the total amount of the administrative fine to be imposed must not exceed this amount.
367. 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 below into its calculations of the individual infringement fines. When the proposed fines for the individual infringements are added together, a total fine with of €240 million arises. The proposed fine is below 2% of the turnover of Meta as considered below.
368. MPIL has argued that the above interpretation and application of Article 83(3) GDPR is incorrect and/or should not be applied because:
- the EDPB WA decision is incorrect as a matter of law and is, in any event, not binding on the DPC;
 - even if the decision were binding on the DPC, it does not require that the DPC impose administrative fines in the manner proposed;
 - the DPC has not had regard to the criteria of effectiveness, proportionality and dissuasiveness in Article 83(1) GDPR when determining the total cumulative proposed fine; and
 - no decision on the correct interpretation of Article 83(3) GDPR should be made prior to the resolution of a challenge of the decision by WhatsApp Ireland.
369. 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.²²²
370. 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

²²² MPIL Submissions on PDD, paras 15.9 and 15.12.

in accordance with this Article in an endeavour to reach consensus.²²³ 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.²²⁴

371. It is not the position of the DPC that the EDPB in and of itself has the power to issue decisions of general application that bind supervisory authorities. The issue is not the powers or functions of the EDPB, but rather the legal responsibility of the DPC to the concerned supervisory authorities, who in themselves happen to be constituent members of the EDPB. In this regard, assistance is provided in the interpretation of the DPC's duties under Article 60(1) GDPR by Recital 123 GDPR, 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 and more broadly its duty of sincere cooperation with fellow EU regulators would be rendered ineffective were it not to ensure, to the best of its ability, such interpretations were applied consistently.
372. 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.
373. 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.²²⁵ MPIL argues that the fine is contrary to the EU law principles of proportionality, *ne bis in idem* and concurrence of laws.²²⁶ The DPC further notes MPIL's submission that overlap between the infringements should be taken into account, in this regard.²²⁷

²²³ Emphasis added.

²²⁴ MPIL Submissions on PDD, paras 15.11.

²²⁵ MPIL Submissions on PDD, paras 15.17 - 15.18.

²²⁶ MPIL Submissions on PDD, paras 15.18.

²²⁷ MPIL Submissions on PDD, paras 15.19.

374. In essence, it is MPIL's view that the proposed fines, either individually or cumulatively, are disproportionate to the circumstances of the case where MPIL considers it made reasonable and diligent efforts to comply with the GDPR, and where MPIL considers the risks to natural persons in connection with the incident to be low. The DPC does not agree with MPIL's assessment, for reasons stated above.
375. MPIL argued that the DPC's approach to imposing cumulative fines in this Inquiry is 'inconsistent' with the EDPB Decision concerning WhatsApp on the basis that 'the EDPB WA Transparency Decision did not direct the DPC to impose separate fines in respect of each infringement and to then add those fines together.' In advancing its alternative interpretation, MPIL has submitted that the principle of *ne bis in idem* applies with regard to the infringements of Articles 25(1) and 25(2) GDPR.²²⁸ For reasons stated at paragraph 349, the DPC does not accept this submission. Similarly, the DPC is not applying a new and retroactive view of wrongdoing to the conduct in a manner envisaged by principle of concurrence of laws. It is simply determining the proper interpretation of Article 83(3) GDPR. This has no impact on the DPC's detailed consideration of MPIL's submissions on the separate and more general question of the appropriate penalty.
376. 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.
377. 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...'.²²⁹ 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.

²²⁸ MPIL Submissions on PDD, paras 12.1 – 12.5.

²²⁹ MPIL Submissions on PDD, para 15.5, footnote 252.

L. ARTICLE 83(4) GDPR

378. Article 83(4) GDPR operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

379. 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...

380. 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.

381. Accordingly, when considering MPIL'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.

382. In this regard, the CJEU has established that:

an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed.²³⁰

383. 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

²³⁰ Case C-41/90 *Höfner and Elser v Macrotron GmbH*, Case C-41/90, EU:C:1991:161, para 21.

the parent company, without having to establish the personal involvement of the parent company in the infringement.²³¹

384. 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.
385. 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.²³²
386. In light of the CJEU’s decision in Case C-516/15 P, *Akzo Nobel and Others v Commission* (‘**Akzo**’), in circumstances where a parent company holds 100%, or almost 100% of shares in a subsidiary company which has infringed Article 83 GDPR, a presumption will arise (the ‘**Akzo presumption**’) that the parent company exercises decisive influence over the subsidiary.
387. The General Court has further held that, in effect, the Akzo 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 a decisive influence over the conduct of its subsidiary.²³³ 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 company²³⁴

²³¹ Case C-97/08 P *Akzo Nobel and Others v Commission* EU:C:2009:536, [2009] ECR I-08237, paras 58-60.

²³² Case C-490/15 P *Ori Martin and SLM v Commission* EU:C:2016:678, para 60.

²³³ Case T-206/06 *Total and Elf Aquitaine v Commission* EU:T:2011:250, [2011] ECR II-00163, para 56; Case T-562/08 *Repsol Lubricantes y Especialidades and Others v Commission* EU:T:2014:1078, para 42; and Cases T-413/10 and T-414/10 *Socitrel and Companhia Previdente v Commission*, EU:T:2015:500, para 204.

²³⁴ Opinion of Advocate General Kokott in Case C-97/08 P *Akzo Nobel and Others v Commission*, EU:C:2009:262, point 73 (as cited in Case T-419/14 *The Goldman Sachs Group, Inc. v European Commission*, Case ECLI:EU:T:2018:445, para 51).

388. The Akzo presumption may be rebutted by the production of evidence relating to the 'organizational, economic and legal links' between the parent and subsidiary to demonstrate that the subsidiary acts independently on the market.
389. It is important to note that 'decisive influence' in this context refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR, in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.
390. As noted above, within the European Region, the Facebook service is provided by MPIL, which is a subsidiary of Meta, and was formerly known as Facebook Ireland Limited. MPIL's ultimate parent is Meta.
391. As noted above, within the European Region, the Facebook service is provided by MPIL. MPIL's ultimate parent company is Meta.
392. 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.

393. 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.

394. 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 2023,²³⁵ notes that MPIL is wholly owned by Facebook International Operations Limited.²³⁶

395. 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 regards its power to (directly or indirectly) exercise a decisive influence over the conduct of MPIL.
396. 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.
397. 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.
398. 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.²³⁷

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.

²³⁵ See paragraph 405 below.

²³⁶ MPIL, 'Companies Registration Office Form B1C – Annual Return General', 30 September 2023.

²³⁷ MPIL Submissions on PDD, para 16.2.

399. 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.²³⁸ The DPC does not agree with this assessment for the following reasons.
400. First, the suggested approach (involving an assessment of where the decision-making power lies, in relation to the processing of personal data) is effectively a replication of the assessment that must be undertaken at the outset of the inquiry process, the outcome of which determines (i) the party/parties to which the inquiry should be addressed; and (ii) (in cross border processing cases) the supervisory authority with jurisdiction to conduct the inquiry. 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.
401. 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".

²³⁸ MPIL Submissions on PDD, para. 16.4.

402. 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.
403. 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.
404. MPIL further submitted that the DPC should refrain from making a decision on this point '...until such time as it has been determined...' ²³⁹ 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 349 above.
405. 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, 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.
406. 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. ²⁴⁰
407. 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 25(1) and Article 25(2) 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 do not exceed the applicable fining cap prescribed by Article 83(4) GDPR.

²³⁹ MPIL Submissions on PDD, paragraph 16.1, footnote 261.

²⁴⁰ Meta Platforms, Inc., Annual Report for year to 31 December 2023, available at <https://investor.fb.com/financials/> (retrieved 20 June 2024).

M. Selection of Amounts of Administrative Fines

408. In having selected from within the fining ranges proposed in the Draft Decision, as set out in Part J of this Decision, the specific amounts of the administrative fines to be imposed in respect of the infringements identified above, the 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 of fine that would be necessary in order to satisfy the requirement for fines to be effective, proportionate and dissuasive.

409. In response to the Article 60 Draft Decision, the FR SA made the following comment:

With regard to the qualification of the breaches, the restricted committee noted that the DPC retained breaches of Articles 25(1) and 25(2) of the GDPR. The restricted committee noticed that the facts described in the draft decision could have been considered as a data processing security breach, based on a breach of Article 32 or Article 5(1)(f) of the GDPR given the vulnerability caused by the modification of the video publishing functionality and the generation of a particular type of access token enabling the attacker to access a user account that was not theirs and, as a result, to target all the friend user accounts linked to it.

With regard to the total amount of the fine envisaged, the restricted committee is sharing the DPC's analysis and is insisting on the seriousness of the breaches observed and the duration of the vulnerability introduced in July 2017, of which META only became aware in September 2018, even though it is certain that META had the technical elements to consider that the modification was not appropriate and should not have been deployed as it stood. Therefore, in view of the particular negligence of the organization, which benefits from substantial technical and financial resources, the restricted committee is considering that the total amount of the fines should be close to the high range proposed, i.e. 240 million euros.

410. 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].

411. 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 conduct 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 Guidelines 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.

Having said this, we would like to point out the details of the Draft Decision concerning the amount of fines:

1. At several points in its elaborations, the DPC has classified the gravity of the infringements with regard to Art. 83 (2) lit. a) GDPR to be of 'medium seriousness' (e.g. para. 285, 288). This might in fact be plausible in view of the duration of the violation (5 months). The number of people affected on the other hand is very high in absolute terms (2,983,092 users affected). This classification therefore appears questionable and we do not agree with the medium seriousness in this respect.

2. The DPC assessed the infringements as negligent (Art. 83 (2) lit. b) GDPR) and considered this element as aggravating due to the degree of negligence (para. 301). The classification in fact appears to be plausible.

3. The DPC took into account the fact that special categories of personal data and children's data were also processed (para. 334). In this respect, the classification as significantly aggravating appears to be absolutely plausible as well.

If these three criteria (Art. 83 (2) lit. a), b) and g) GDPR) are considered altogether, the classification of the severity of the violations as 'medium' could be justifiable.

According to the Guidelines 04/2022, this would result in the following starting amount for the calculation:

10% - 20% 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 € 243.1 million and € 486.3 million.

According to the Guidelines, the next step after determining a starting amount, would be to deduct or add amounts for any mitigating and aggravating factors. The DPC has assessed the measures taken to mitigate the damage (Art. 83 (2) lit. c) GDPR, para. 315) and all other aggravating/mitigating circumstances (Art. 83 (2) lit. k), para. 340) as mitigating factors.

After all, the DPC proposes a total fine in the range of minimum € 170 million and maximum € 240 million. This result certainly is not implausible. However, it appears to be at the very bottom end of the possible scale. In our view, it might be justified to take the following factors of the DPC's assessment into account as more aggravating factors:

- The fact that a very high number of users were affected by MPIL's violations, namely 2,983,092 users.
- The level of negligence that the DPC attributed to MPIL.

- The fact that special categories of personal data and children's data were also disclosed in connection with MPIL's violations.

In addition, 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.

412. 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.
413. 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.
414. 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 CJEU²⁴¹ and Irish Courts²⁴² in this regard.

415. The DPC agrees with this analysis of its obligation to 'take due account' of CSAs' comments under Article 60(3) GDPR.
416. 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 earlier positions including as follows:
- i. The relationship between the facts on which the DPC has found infringements of Articles 25(1) and 25(2) GDPR mean that MPIL 'is being punished twice for the same alleged wrongdoing',
 - ii. the higher ends of the fining ranges proposed in the Draft Decision are disproportionate and penal when compared to fines imposed by the DPC and other supervisory authorities for data breaches 'including in far more serious cases'.
 - iii. the DPC has misinterpreted and misapplied the factors listed in Article 83(2) GDPR,
 - iv. the DPC has not given sufficient weight to MPIL's mitigation actions,
 - v. the DPC has mischaracterised and wrongly attributed importance to the categories of personal data affected by the personal data breach,
 - vi. the DPC incorrectly took account of Meta's global turnover when determining the ranges of fines proposed in the Draft Decision, and
 - vii. the DPC has misconstrued Article 83(3) by not restricting fines to that proposed for infringement of Article 25(1), being the infringement that the DPC considers the gravest.

In circumstances where the DPC has already addressed these matters, it is not necessary to repeat its position on them here.

²⁴¹ Case C-349/07 *Sopropé v Fazenda Pública* EU:C:2008:746, para 50.

²⁴² *Mahon v Keena* [2009] IESC 64.

417. 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*,²⁴³ 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.

418. 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.
419. 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 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.
420. 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’.
421. 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

²⁴³ Case C-683/21 *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija* EU:C:2023:949.

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.

422. 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, their duration and the resources available to Meta that should have enabled it to appreciate the inappropriate nature of the coding changes that led to the breach, 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 imposed 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.
423. 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.

N. SUMMARY OF CORRECTIVE POWERS

424. In summary, the corrective powers that the DPC has decided to exercise are:
- (1) a Reprimand to MPIL pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and
 - (2) two administrative fines, as follows:
 - (a) In respect of MPIL's infringement of Article 25(1) GDPR, a fine of €130 million.
 - (b) In respect of MPIL's infringement of Article 25(2) GDPR, a fine of €110 million.

425. MPIL has the right of an effective remedy as against this Decision, the details of which have been provided separately.

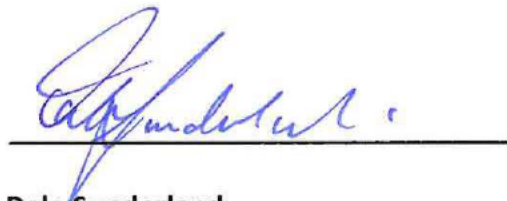
This Decision is addressed to:

**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**

O. Appendix: Categories of data affected by the Infringement

Category	Data Affected
1	Basic profile information: full name, email address, and phone number (if there was one associated with the account)
2	<p>In addition to the basic profile information mentioned above, additional profile information mentioned was also obtained. Specially the following information fields may have been obtained (to the extent that information was held in such fields following activity, or provision of information, by the user):</p> <ul style="list-style-type: none"> a. username, b. first name used on the profile c. last name used on the profile, d. name [nickname as set by the user on the profile (if any), e. email address [primary email address associated with the account], f. phone [confirmed mobile phone numbers associated with the account], g. gender [as set by the user on the profile], h. locale [language as picked by the user], i. relationship status [as set by the user on the profile], j. religion [as described by the user on the profile], k. hometown [as set by the user on the profile], l. location [current city, as set by the user on the profile], m. birthday [as set by the user on the profile], n. devices [that are used by the user to access Facebook - fields include 'os' (e.g. iOS) and hardware (e.g. iPhone)], o. educational background [as set by the user on the profile FB], p. work history [as set by the user on the profile FB], q. website [list of URLs entered by the user into the website field on FB profile], r. verified [this is a flag for whether Facebook has a strong indication that user is who they say they are], s. 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], t. recent search queries on Facebook, u. up to the top 500 accounts that the user follows.
3	<p>In addition to information set out in 1 and 2, above, further information may have been exposed due to the blunt force nature of the attack on these accounts. In addition to the types of information already mentioned above, the attack involved the rendering of the full profile/timeline of many of these users, thereby incidentally exposing the raw HTML source for those pages. This includes posts on their timeline, their list of friends, Groups they are members of, and the names of recent Messenger conversations. Message content was not available to attackers, with one exception: if a person in this group was a Page admin whose Page had received a message from someone on Facebook, the content of that message was available to the attackers. This information would not necessarily have been complete or available to the attackers in a structured form, rather it would have been as incidental inclusions in the HTML text that included the access token and was not separately requested via additional API queries.</p>