In the matter of the General Data Protection Regulation

DPC Case Reference: IN 18-11-5

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 Regulaltion

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

DECISION

Decision-Maker for the Commission:

Helen Dixon

Commissioner for Data Protection

Dated the 15th day of March 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

INTRODUCTION

1. This is the decision (**"the Decision"**) of the Data Protection Commission (**"the DPC"**), made pursuant to Section 111 of the Data Protection Act, 2018 (**"the 2018 Act"**) and in accordance with Article 60 of Regulation (EU) 2016/679 (General Data Protection Regulation) (**"the GDPR"**), arising from an inquiry conducted by the DPC of its own volition under Section 110(1) of the 2018 Act (**"the Inquiry"**).

2. The Inquiry was commenced on 11 December 2018 in respect of twelve personal data breaches (**"the Breaches"**) which were notified to the DPC by or on behalf of Facebook Ireland Limited (**"FB-I"**) on dates between 7 June 2018 and 4 December 2018. While Facebook Ireland Limited has since changed its name to Meta Platforms Ireland Limited, with effect from 5 January 2022, the relevant events, for the purpose of the Inquiry, occurred prior to this name change. In the circumstances, the term "FB-I" is used throughout this Decision to denote Meta Platforms Ireland Limited, the company formerly known as Facebook Ireland Limited. Similarly, Facebook, Inc. changed its name to Meta Platforms, Inc. on 28 October 2021 and any references, within this Decision, to "Facebook, Inc." should be understood as meaning Meta Platforms, Inc., the company formerly known as Facebook, Inc.

3. This Decision sets out my findings, as the decision-maker for the DPC in this matter, as to whether (i) an infringement of a relevant enactment by FB-I, the controller to which the Inquiry relates, has occurred or is occurring, and (ii) if so, whether a corrective power should be exercised in respect of FB-I as the controller concerned, and the corrective power that is to be so 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.[1]

4. For the avoidance of doubt, this Decision represents the collective views of the Commission and supervisory authorities concerned[2] ("**CSAs**", each one being a "**CSA**"), further to the co-decision-making process outlined in Article 60 GDPR.

PRELIMINARY MATTERS

Controller and processor

5. This Decision is addressed to Meta Platforms Ireland Limited, a private company limited by shares with registered offices at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. As already noted above, Meta Platforms Ireland Limited became the new name of Facebook Ireland Limited, effective 5 January 2022. Each of the breach notifications[3] submitted to the DPC in respect of the Breaches were submitted by or on behalf of FB-I as a controller within the meaning of Article 4(7)

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

[2] As defined in Article 4(22) GDPR.

[3] References in this Decision to breach notifications are references to notifications made via the DPC's Cross-Border Breach Notification Form, used to facilitate controllers in making personal data breach notifications involving cross-border processing within the meaning of Article 4(23) GDPR. Between 7 June 2018 and 4 December 2018, the Cross-Border Breach Notification Form was available for download on the DPC's website, and the completed form submitted by email to the DPC with a self-declared 'risk rating' in the subject line, indicating whether the controller considered the personal data breach to be 'Low Risk', 'High Risk', 'Medium Risk', or 'Severe Risk'. Due to revisions to the Cross-Border Breach Notification Form in that time period, six of the Breaches (Breach 7, Breach 8, Breach 9, Breach 10, Breach 11, and Breach 12) were made using a newer version of the form. Those six breach notifications were also accompanied by a copy of FB-I's record of processing activities for the purpose of Article 30 GDPR.

GDPR. FB-I had confirmed to the DPC previously by email dated 25 May 2018 that FB-I was the controller for the Facebook service and the Instagram service in the EU. It is understood that FB-I is also the controller for the provision of the Facebook and Instagram services to users in the other EEA states (Norway, Liechtenstein and Iceland).[4] In the Inquiry, FB-I specifically stated that, as controller, it determines the purposes and means of processing of the personal data of EU users[5] which I assume to include users in the other EEA states.

6. Facebook, Inc. (as it was then known) 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. FB-I has confirmed in the Inquiry that Facebook, Inc. acted as a processor as defined in Article 4(8) GDPR in relation to the data processing concerned by each of the Breaches.[6] In this regard, FB-I has outlined that Facebook, Inc. processes the personal data of EU users of the Facebook and Instagram services solely on FB-I'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. [7] A copy of the DTPA was provided to the DPC in the Inquiry.

7. I am satisfied, for the purposes of this Decision, that FB-I and Facebook, Inc. are appropriately identified as the controller and processor, respectively, for the processing of personal data the subject of the Inquiry.

Facebook and Instagram

8. The Breaches to which the Inquiry relates concern both the Facebook and Instagram services.

9. Facebook is a social media service available at the website www.facebook.com, and as an app for Android and iOS. As of the end of December 2018, it had 2.32 billion monthly active users globally.[8] In very broad overview, 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' and 'Groups' and 'Events' around particular interests, topics, or social activities. The homepage 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 who 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.

---

[4] See, for example, information on users affected, including numbers in the other EEA states, in the updated breach notification form for Breach 10 (4 January 2019) (Section 8.1, updating Section 5.5).
[5] FB-I's Response to Queries 1 to 4 in the Commencement Notice (18 January 2019), pages 1 to 2.
[6] FB-I's Response to Queries 1 to 4 in the Commencement Notice (18 January 2019), page 3 to 4
[7] FB-I's Response to Queries 1 to 4 in the Commencement Notice (18 January 2019), page 4.
[8] Press Release, 'Facebook Reports Fourth Quarter and Full Year 2018 Results' (30 January 2019) <https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx>.

10. Instagram is a social media service available as an app for Android and iOS and at the website www.instagram.com. Instagram was acquired by Facebook, Inc. in 2012, and in June 2018 had more than one billion active monthly accounts globally.[9] Users can create an account and profile to avail of a variety of sharing and communication features. These include, for example, posting or sharing photos, videos, and locations, 'following' other users, commenting on or 'liking' posts, 'tagging' or 'mentioning' people in photos or videos, sending messages to other users or groups of users, and sharing photos and videos via a 24-hour 'Instagram Story'. Accounts can be 'public' (where anyone can see the user's posts or profile on Instagram) or 'private' (where the user manages who sees the user's photos and profile by approving follower requests from other users). Professional 'Business Accounts' are also available as 'public' accounts only. A person can 'block' another user if, for example, they wish to remove that user's likes and comments from photos or videos they post, or no longer wish to receive messages from that user.

11. Facebook and Instagram accounts are available to both adults and children. Users are required under the Terms of Service[10] to be at least 13 years old to use both Facebook and Instagram.[11]

Competence of the DPC as lead supervisory authority

12. Chapter VI, Section 2 of the GDPR deals with the competence, tasks and powers of the supervisory authorities. Article 55(1) GDPR provides that each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with the GDPR on the territory of its own Member State. Article 56(1) GDPR states:

> *"Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."*

13. The concept of the "*main establishment*" of a controller is defined in Article 4(16)(a) GDPR to mean:

> *"as regards a controller with establishments in more than one Member State, 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."*

14. FB-I has confirmed that it is the service provider of its services in the EU and that it determines the means and purposes of processing of EU users' personal data. FB-I has further confirmed that it is the only entity with decision-making power regarding:

- Setting policies governing how EU user data is processed;

---

[9] Facebook for Business, 'How to connect with new audiences on Instagram' (31 January 2019), available at <https://www.facebook.com/business/news/insights/how-to-connect-with-new-audiences-on-instagram>.
[10] Facebook and Instagram's Terms of Service are available as of August 2021 at <https://www.facebook.com/terms> and <https://help.instagram.com/581066165581870/>, respectively.
[11] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 20.

- Deciding whether and how any product that involves the processing of user data will be offered in the EU;

- Controlling the access to, and use of, EU user data; and

- Handling and resolving data-related inquiries and complaints from European users of the Service, whether directly or indirectly, via regulators.

15. I note that the above affirmation of controllership is contained in FB-I's privacy policy. I also note that FB-I's Dublin office constitutes Facebook's European headquarters. FB-I, as at 27 January 2022, had approximately [redacted] direct employees and several thousand further indirect employees working for its Dublin office. Amongst these employees are key data protection personnel, including FB-I's Head of Data Protection and Associate General Counsel.

16. Further, there has been a course of historical and ongoing engagement, by FB-I, with the DPC's Consultation Unit (through which the DPC carries out its supervision function), dating back a number of years and predating the application of the GDPR. This engagement has been conducted in relation to the handling of complaints, amongst other things. By way of a specific recent example, the DPC attended at FB-I's Dublin office in order to inspect documents relating to the (then) proposed roll-out of a new dating feature. This roll-out was delayed as a result of concerns expressed by the DPC about the extent of compliance of the feature with the GDPR. In the context of this inspection, it was clear that decisions in relation to this data processing were made by FB-I, just as other such decisions have been made in the past and are made on a daily basis by FB-I. Having regard to these ongoing interactions, the DPC is satisfied that FB-I acts as the controller, determining the means and purposes of processing in respect of the personal data of individuals, in relation to the delivery of its services across the EU.

17. I am satisfied, in light of the above and the information provided by FB-I in the breach notifications and in the course of the Inquiry, that FB-I's establishment in Ireland is its place of central administration in the EU, and that the decisions on the purposes and means of the processing of personal data of EU users of the Facebook and Instagram services are taken there. FB-I accordingly has its "*main establishment*" within the meaning of Article 4(16) GDPR in Ireland. FB-I confirmed in the Inquiry that it was engaged in cross-border processing in respect of the data processing pertaining to each of the Breaches pursuant to Article 4(23) GDPR.[12]

18. In light of the above, I consider that the DPC 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.

Case reference numbers

19. The DPC assigned internal case reference numbers to each of the Breaches as they were notified, which were used by the DPC throughout the Inquiry. For clarity, I will refer to the Breaches by numbers 1 to 12 in the order in which they were first notified to the DPC, as follows:

Case reference	Date notified	Designation
BN-18-6-77	7 June 2018	"Breach 1"
BN-18-6-306	16 June 2018	"Breach 2"

[12] FB-I's Response to Queries 1 to 4 in the Commencement Notice (18 January 2019), page 1.

BN-18-6-494	23 June 2018	**"Breach 3"**
BN-18-7-38	30 June 2018	**"Breach 4"**
BN-18-7-163	5 July 2018	**"Breach 5"**
BN-18-7-363	14 July 2018	**"Breach 6"**
BN-18-8-67	2 August 2018	**"Breach 7"**
BN-18-8-344	17 August 2018	**"Breach 8"**
BN-18-8-345	19 August 2018	**"Breach 9"**
BN-18-11-332	22 November 2018	**"Breach 10"**
BN-18-12-22	3 December 2018	**"Breach 11"**
BN-18-12-39	4 December 2018	**"Breach 12"**

BACKGROUND

Overview

20. A general overview[13] of each of the twelve Breaches is set out in **Schedule 1** to this Decision. Seven of the Breaches related to the Facebook service only, three of the Breaches related to the Instagram service only, and two of the Breaches concerned both Facebook and Instagram.

21. I am satisfied, in light of the information provided by FB-I in the Inquiry, that each of the Breaches constituted personal data breaches within the meaning of Article 4(12) GDPR, to which the notification obligation under Article 33(1) GDPR applied. Each of the Breaches were notified to the DPC further to FB-I's obligations as a data controller under Article 33 GDPR. Notifications to affected data subjects were made by or on behalf of FB-I in respect of Breaches 1, 2, 7, 10, 11, and 12. In each case, FB-I indicated that the notification to data subjects was made *"voluntarily"*, rather than pursuant to Article 34 GDPR (which requires mandatory notification of data subjects where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons). At the time they were notified to the DPC, Breaches [redacted] were described by FB-I as "*Medium Risk*". Breaches [redacted] were each described by FB-I as "*Low Risk*".

22. The Breaches were caused by software bugs (and, in the case of Breach 12 only, a server misconfiguration) affecting the Facebook and Instagram services, giving rise to incidents constituting personal data breaches within the meaning of Article 4(12) GDPR. With the exception of Breach 7, in general, the Breaches affected the confidentiality of personal data (i.e. involved a breach of security leading to an unauthorised disclosure of, or access to, personal data). Breach 7 affected the availability of personal data (i.e. involved an accidental or unlawful loss or destruction of personal data).

23. The nature of the personal data concerned differed depending on the circumstances of the Breach. Several of the Breaches related to personal data comprising, or contained in, posts, Stories, videos or photos posted to Facebook or Instagram by EU users. By way of further example, Breach 9 concerned messages sent between Instagram users, Breach 10 involved access to users' Facebook photos by third-party apps, and Breaches 3 and 5 concerned information identifying the Page Admins of Facebook pages.

[13] For clarity, the information contained in the table in **Schedule 1** is for the purpose of providing a convenient summary of the Breaches by way of background to the Inquiry and the issues for determination in this Decision. It is not a full overview of all of the information provided by FB-I in respect of each of the twelve Breaches during the course of the Inquiry.

Number of EU users potentially affected by each of the Breaches

24. The DPC requested that FB-I provide information as to the number of EU users affected by each of the Breaches. The figures provided by FB-I are set out below. In each case, the figure provided represents the *upper limit or ceiling* of the number of EU users[14] FB-I estimated to be potentially affected.[15] FB-I has further clarified that it considers the numbers provided to represent estimates of the upper limit or ceiling of EU users "concerned" in relation to the Breaches within the meaning of Article 33(3)(a) GDPR, and disputes that those data subjects were necessarily "affected" by the Breaches.[16] FB-I provided breakdowns of the number of EU users affected by country in respect of Breaches [redacted]

Breach 1[17]	[redacted]
Breach 2[18]	
Breach 3	
Breach 4[19]	
Breach 5	
Breach 6[20]	
Breach 7[21]	
Breach 8[22]	
Breach 9[23]	
Breach 10[24]	
Breach 11[25]	
Breach 12[26]	

CONDUCT OF THE INQUIRY

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

Notifications and Updates

26. As set out above, each of the Breaches at issue were notified to the DPC on dates between 7 June 2018 and 4 December 2018. FB-I continued to supply information and documentation relating to the breaches after making the notifications. The first of the updates, which related to Breach 1, was supplied on 2 July 2018. The latest, which concerned Breach 3, was provided on 24 January 2020.

[14] In some instances these figures include the numbers of users in the other EEA states (Iceland, Liechtenstein and Norway) affected by the Breaches for whom FB-I is also a controller.
[15] FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 20 to 21.
[16] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraph 1.3, page 8.
[17] Updated breach notification form for Breach 1 (2 July 2018) (Section 9).
[18] Updated breach notification form for Breach 2 (14 August 2018) (Section 9).
[19] Updated breach notification form for Breach 4 (19 September 2018) (Section 9, updating Section 8.3B).
[20] Updated breach notification form for Breach 6 (20 September 2018) (Section 9, updating Section 8.3B).
[21] An email update for Breach 7 dated 14 September 2018, while not confirming the exact numbers, indicated that Breach 7 "*affected* [redacted] *of users across the EU*".
[22] Updated breach notification form for Breach 8 (19 September 2018) (Section 8.1).
[23] Updated breach notification form for Breach 9 (19 September 2018) (Section 8.1).
[24] Updated breach notification form for Breach 10 (4 January 2019) (Section 8.1).
[25] Breach notification form for Breach 11 (3 December 2018) (Sections 5.3 to 5.5).
[26] Updated breach form for Breach 12 (4 January 2019) (Section 8.1).

The updates included further information and documentation relating to the personal data breaches, supplied on a phased basis as envisaged by Article 33(4) GDPR.

Commencement Notice and Responses

27. The Inquiry was commenced by letter dated 11 December 2018 (**"the Commencement Notice"**) under Section 110(1) of the 2018 Act, of the DPC's own volition. The rationale for commencing the Inquiry was based on concerns the DPC had formed in respect of the Breaches, all twelve of which had been notified to the DPC on dates between 7 June 2018 and 4 December 2018.

28. Having reviewed the information provided by FB-I in connection with each of the Breaches in the breach notifications and associated updates in the period between June and December 2018, the DPC formed the view that it was appropriate to assess the subject matter of the Breaches in the context of an inquiry under Section 110(1) of the 2018 Act, in order to ascertain whether an infringement of the 2018 Act or the GDPR had occurred, or was occurring.

29. The Commencement Notice in the Inquiry included an Appendix containing a list of 15 queries (certain of which were divided into sub-queries) addressed to establishing the facts as they related to the subject matter of the Inquiry. Queries 4, 5, 8, 9, 10, 11, 12, 13, 14 and 15 requested relevant supporting documentary evidence. FB-I was specifically informed in the Appendix to the Commencement Notice that, where relevant supporting documentary evidence was requested in the queries, FB-I was being asked to provide:

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

30. Following correspondence between FB-I and the DPC during late December 2018 and early January 2019 in relation to the deadline for receiving the information requested in the Commencement Notice, FB-I's responses to the 15 queries (**"the Responses to Queries in the Commencement Notice"**) were provided in 8 phases in accordance with an agreed timetable for phased responses ending on 15 March 2019.

Correspondence concerning Expert Review

31. Query 8 in the Commencement Notice required FB-I to provide detailed information, and relevant supporting documentary evidence, regarding any technical and organisational weaknesses FB-I had identified that may have contributed to all or any of the Breaches. In its Response to Queries 5 to 12 in the Commencement Notice (Breach 1 and 2) (26 January 2019), FB-I informed the DPC, in reply to Query 8, that it was in the process of commencing a technical and organisational measures review (**"the Expert Review"**) and would be instructing an expert technologist in that regard.

32. On 30 January 2019, the DPC wrote to FB-I, requesting clarification and relevant supporting documentation, in relation to the Expert Review referred to by FB-I by close of business on 8 February 2019. FB-I replied by letter dated 7 February 2019, indicating that, as of 4 February 2019, an expert technologist had been engaged by FB-I's external lawyers:

> *"on a privileged basis (in light of the Inquiry and other actual, threatened and/or contemplated regulatory inquiries / litigation [FB-I] is facing). As indicated in our responses dated 26 January 2019, however, [FB-I] will endeavour to update the*

DPC in relation to the outcomes of [the expert technologist's] review, as appropriate."

33. By email dated 2 May 2019, FB-I provided further information by way of update in relation to the Expert Review. FB-I indicated (without prejudice to its privileged nature) that the scope of the Expert Review would cover: (i) in its first phase, FB-I's incident response plans and policies, its notification, documentation and record-keeping practices associated with personal data breaches and the implementation of same in relation to a number of the Breaches in the Inquiry; and (ii) in its second phase, FB-I's data security measures and security policy documentation.

34. The DPC replied by email dated 2 May 2019, seeking clarification as to whether FB-I intended to provide the DPC with a full copy of the report of the Expert Review, and, if not, what information FB-I intended to provide to the DPC following its completion. FB-I responded on 9 May 2019, reiterating that the Expert Review was privileged and that, while FB-I would endeavour to update the DPC in relation to the review where possible and appropriate, FB-I could not detail what information it would be able to provide to the DPC in this regard, or when FB-I would be able to do so.

35. FB-I provided an update to the DPC following the completion of the Expert Review by way of letter dated 23 March 2020, detailing, in overview (and without prejudice to its privileged nature), the scope of the review and the measures FB-I proposed to implement on foot of it. This letter dated 23 March 2020 informed the DPC that a review of Facebook, Inc.'s coding practices was also carried out as part of the Expert Review. The DPC was not provided with a copy of any report arising from the Expert Review. Further information in relation to the Expert Review was provided in FB-I's Response to the Draft Inquiry Report (22 May 2020) (in particular pages 47 to 51 and Annex 3 and Annex 4 thereof). Annex 3 consisted of a document entitled '[redacted]' dated [redacted] The documentation comprising Annex 4 to was provided to the DPC separately on 9 June 2020.

Additional Queries and Responses

36. By letter dated 5 June 2019, the DPC wrote to FB-I with 10 further queries relating to matters arising from the information FB-I had provided in its Responses to the Commencement Notice. FB-I was requested to provide relevant supporting documentary evidence with its replies. FB-I provided responses to these queries (**"the Responses to the Additional Queries"**) on 14 June 2019.

Draft Inquiry Report and Response

37. FB-I had previously been informed that the scope of the Inquiry would include an examination of FB-I's compliance with Articles 5, 24, 25, 28, 29, 32, 33 and 34 GDPR in connection with the Breaches.[27] The inquiry team wrote to FB-I by letter of 15 August 2019 for the purpose of setting out the principal issues that would be the subject of consideration in the draft inquiry report (**"the Draft Inquiry Report"**), and inviting FB-I's views on same. The principal issues identified in Appendix A to the letter dated 15 August 2019 were narrowed to an examination of FB-I's compliance with Article 5(1)(f) and 5(2), 24, and 32 GDPR. FB-I duly provided its observations in respect of the principal issues by letter dated 30 August 2019.

38. The DPC issued its Draft Inquiry Report to FB-I on 21 April 2020. FB-I (through its legal representatives) provided submissions in response to same on 22 May 2020 (**"the Response to the**

[27] Letters from the DPC to FB-I dated 21 December 2018 and 9 January 2019.

Draft Inquiry Report"), with certain supplemental materials comprising Annex 4 provided on 9 June 2020. In a letter dated 9 June 2020, the DPC indicated its willingness to receive any further submission or documentation FB-I might wish to provide by a deadline of 19 June 2020. On 17 June 2020, FB-I's legal representatives indicated that FB-I did not wish to provide any further submissions in the Inquiry at that time.

Final Inquiry Report and Decision-Making Stage

39. The Final Inquiry Report was forwarded to me as the decision-maker on 2 December 2020. I notified FB-I's legal representatives of the commencement of the decision-making stage in the inquiry by letter dated 18 February 2021 and a copy of the Final Inquiry Report was provided to FB-I's legal representatives, for information purposes, on 22 February 2021.

40. For the purpose of enabling me to carry out my decision-making function, the inquiry team provided to me, along with the Final Inquiry Report, copies of all of the documentation annexed to the Final Inquiry Report, including copies of the breach notification forms submitted by FB-I to the DPC in respect of each of the Breaches and any updates thereto, copies of all of the responses submitted by FB-I in the Inquiry and the documentation annexed to same, the Draft Report and FB-I's Response to the Draft Report, and copies of all relevant correspondence exchanged between FB-I and the DPC in the Inquiry.

41. I provided FB-I with my preliminary draft decision in this matter on 8 June 2021 ("the Preliminary Draft Decision") for the purpose of enabling FB-I to make submissions as to my provisional findings and proposed exercise of corrective powers as outlined in that preliminary draft. FB-I provided its substantive submissions ("the Response to the Preliminary Draft Decision") on 21 July 2021.

42. I am satisfied that I have received all relevant materials necessary for me to perform my decision-making function in respect of this Inquiry. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the inquiry team, as well the submissions made by FB-I on the Preliminary Draft Decision, and any other information which I consider to be relevant to my decision.

43. Having taken account of FB-I's Response to the Preliminary Draft Decision, I finalised and circulated a draft decision to the CSAs on 18 August 2021 ("the Article 60 Draft"). Given that the matters under examination in the within inquiry entail cross-border processing throughout Europe, all other supervisory authorities were engaged as CSAs for the purpose of the co-decision-making process outlined in Article 60 GDPR. Objections to the Article 60 Draft were raised by the supervisory authorities of Hamburg and Poland. In addition, comments were exchanged by the supervisory authorities of France, the Netherlands, Baden-Württemberg, Hungary and Portugal. Having engaged with the CSAs and FB-I in relation to the subject-matter of the objections and comments, I further amended the Article 60 Draft and circulated it to the CSAs on 8 February 2022 for the purpose of Article 60(5) GDPR ("the Amended Article 60 Draft"). Following the expiry of the prescribed two week consultation period, and having achieved consensus with the CSAs on the matters arising, the DPC adopted this Decision on the basis of the Amended Article 60 Draft.

Fair procedures

44. Having reviewed the correspondence in the Inquiry (including those representations made by FB-I specifically directed to the fairness of the procedures adopted by the DPC[28] and the DPC's replies to same[29]) I am satisfied that the Inquiry was correctly conducted and that fair procedures were afforded to FB-I by the DPC throughout. This includes, but is not limited to, the steps taken by the DPC to: (i) notify FB-I of the issues under examination in the Inquiry and the information and documentation required by the DPC, (ii) provide FB-I with an opportunity to provide responses and submissions in respect of the issues under consideration in the Inquiry at appropriate stages, and (iii) provide FB-I with sufficient time (including extensions of time, where necessary) to furnish the information and documentation requested by the DPC during the course of the Inquiry.

ISSUES AND SCOPE

45. The following issues arise in this Decision:

    (1) Whether FB-I complied with Article 32(1) GDPR and, in particular, Articles 32(1)(b) and (d), with reference to the processing of personal data relevant to the twelve Breaches concerned by the Inquiry in the period between 7 June 2018 and 4 December 2018.

    (2) Whether FB-I complied with Article 24(1) GDPR with reference to the processing of personal data relevant to the twelve Breaches concerned by the Inquiry in the period between 7 June and 4 December 2018. This includes consideration of whether FB-I implemented appropriate data protection policies as envisaged by Article 24(2) GDPR.

    (3) As required by Article 5(1)(f) and Article 5(2) GDPR, whether FB-I was able to demonstrate that the personal data relevant to the twelve Breaches concerned by the Inquiry in the period between 7 June 2018 and 4 December 2018 was processed in a manner that ensured 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.

46. Arising from the analysis in relation to the issues referred to above, I will later consider whether a corrective power should be exercised in respect of FB-I as the controller concerned, and the corrective power that is to be so exercised.

47. Consistent with the material scope of Inquiry notified to FB-I by letter dated 15 August 2019, and with the issues examined in the Draft Inquiry Report and Final Inquiry Report, this Decision is solely addressed to FB-I's compliance with Article 5(1)(f), 5(2), 24 and 32 GDPR in the context of the twelve Breaches.

48. In addition, as set out previously, each of the twelve Breaches giving rise to this Inquiry were notified to the DPC between 7 June 2018 and 4 December 2018. The temporal scope of the findings which follow in relation to FB-I's compliance with the GDPR relate to that period and, in examining FB-I's compliance with Articles 5(1)(f), 5(2), 24 and 32 GDPR, the focus is on the appropriateness of the measures FB-I had in place at that time. This Decision is not concerned with, and does not address, FB-I's compliance with the GDPR presently, in 2022. This is without prejudice to the need for the DPC

[28] Including letters from FB-I to the DPC dated 30 January 2019, 7 June 2019, and 22 May 2020.
[29] Including letters from the DPC to FB-I dated 24 June 2019 and 9 June 2020.

to take into account events relevant to the factual chronology of the twelve Breaches concerned in the Inquiry which occurred at times prior to 7 June 2018 or after 4 December 2018 which are material to the issues for determination in this Decision.

ANALYSIS

Relevant provisions of the GDPR

49. Article 32(1) GDPR provides:

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

50. Article 32(2) GDPR is relevant to the interpretation of Article 32(1) and further provides:

> *"2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."*

51. Recitals 75, 76, 83 and 85 GDPR also provide important guidance that assist in the interpretation of Article 32 GDPR.

52. Article 32 GDPR is closely associated with the 'integrity and confidentiality' principle outlined in Article 5(1)(f) GDPR, which 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')"*

53. Article 5(2) GDPR provides that "*[t]he controller shall be responsible for, and be able to demonstrate compliance with, [Article 5(1)] ('accountability')*". This includes accountability in respect of the 'integrity and confidentiality' principle in Article 5(1)(f) GDPR.

54. The requirement for accountability on the part of controllers in relation to compliance with the GDPR is further detailed in Article 24 GDPR, which states:

> *"1. Taking into account 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, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*
>
> *2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*
>
> *3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller."*

55. Recitals 74 to 78 are especially relevant to the interpretation of Article 24 GDPR. In particular, Recital 74 GDPR states that:

> *"The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."*

Analysis of risks of processing for the purpose of providing the Facebook and Instagram services, taking into account its nature, scope, context and purposes in the context of Articles 24(1) and 32(1) and (2) GDPR

56. Article 32(1) GDPR provides that a controller should "*implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*" associated with the processing of personal data by the controller and processor. Article 32(1) specifically requires the "*risk of varying likelihood and severity for the rights and freedoms of natural persons*" to be taken into account. Article 32(2) further requires that in assessing the appropriate level of security in the context of Article 32(1), account shall be taken of the risks that are presented by processing, in particular from "*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*" (i.e. personal data breaches as defined in Article 4(12) GDPR). Risk to the rights and freedoms of data subjects is also a matter to be taken into account by controllers under Article 24(1) GDPR.

57. The European Data Protection Board (**"EDPB"**) has explained the concept of "*appropriate*" technical and organisational measures as follows:

> *"Technical and organizational 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 should be suited to achieve the intended purpose, i.e. they*

must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness."[30]

58. Recitals 75 and 76 provide guidance as to how risk should be assessed in the context of the GDPR in general. In particular, Recital 76 indicates that:

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

59. The Breaches the subject of this Inquiry highlight, in particular, the risk of software bugs occurring in the codebase underlying Facebook, Inc.'s systems, resulting in personal data breaches within the meaning of Article 4(12) GDPR. FB-I has submitted that the occurrence of software bugs is an "*inherent risk*", particularly in a large and complex codebase such as that which underlies the Facebook and Instagram services.[31] I acknowledge that "*perfect security*"[32] is not the standard set by the GDPR. Rather, controllers are required to implement appropriate technical and organisational measures to ensure *a level of security appropriate to the risk*. In this context, FB-I is required to implement and demonstrate appropriate technical and organisational measures to effectively limit the likelihood of software bugs occurring. I consider it appropriate to have regard to the fact that this Inquiry arises from the notification to the DPC of twelve personal data breaches affecting the Facebook and Instagram services in a period of approximately six months between 7 June 2018 and 4 December 2018, which I consider to be relatively frequent in respect of that period. I wish to specifically state, however, in agreement with the inquiry team,[33] that I do not take the view that the frequency of the Breaches can be taken to conclusively indicate systemic flaws in FB-I's technical and organisational security measures.

60. In relation to the *nature, scope, context, and purposes of the processing*, I consider it relevant to have regard to the following matters:

(1) Facebook and Instagram are popular and widely used social media services. As of the end of December 2018, Facebook had 2.32 billion monthly active users globally,[34] and as of June 2018, Instagram had more than one billion active monthly accounts globally.[35] Further, FB-I has confirmed that in Q4 2018, when this Inquiry commenced, the Facebook service (including, for these purposes, Facebook Messenger) had [redacted] million monthly active users in the EU.[36] FB-I

---

[30] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (20 October 2020), page 6. The relation of appropriateness and effectiveness in this context is also underlined in Recital 74 GDPR.

[31] FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 11 to 14.

[32] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 11.

[33] Final Inquiry Report (2 December 2020), page 106.

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

[35] Facebook for Business, 'How to connect with new audiences on Instagram' (31 January 2019), available at <https://www.facebook.com/business/news/insights/how-to-connect-with-new-audiences-on-instagram>.

[36] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraph 1.2 and footnote 20, page 8. FB-I has explained that it defines a monthly active user of the Facebook service as a registered Facebook user who logged in and visited Facebook through the website or a mobile device, or used the Facebook Messenger application (and is also a registered Facebook user), in the last 30 days as of the date of measurement. This figure consists of active accounts rather than unique users and therefore includes "duplicate" and "false" accounts.

also confirmed that, in Q4 2018, the Instagram service had [redacted] million monthly active users in the EU.[37]

(2) FB-I has submitted that the Facebook and Instagram services are unique in their nature, scope, complexity and scale, and that "the enormous codebase of FB-I's processor [Facebook] Inc., provides a broad range of services to billions of users of [Facebook and Instagram] around the world, including (under [FB-I's] controllership) hundreds of millions in the European region."[38] In view of the information provided by FB-I in the Inquiry, the processing involved in providing the Facebook and Instagram services to EU users is clearly on a vast scale.

(3) The processing carried out for the purpose of providing the Facebook and Instagram services involves large numbers of data subjects, as well as a wide range of types and categories of personal data (potentially including children's data and special category data in some circumstances) in high volumes. This may be appreciated from the record of processing activities for the purpose of Article 30 GDPR supplied by FB-I in the Inquiry,[39] the variety of social media and networking features and content EU users interact with on both Facebook and Instagram, and the acknowledgement on the part of FB-I that it is responsible as a controller for hundreds of millions of EU users of the Facebook and Instagram services. Furthermore, in light of the estimated numbers of data subjects involved in the twelve Breaches (an estimated *upper ceiling* of approximately [redacted]) and the characteristics of the processing involved in the Facebook and Instagram services previously outlined, which is likely to include information on users' daily lives and interests, I consider it relevant that the wide range of types and categories of personal data concerned potentially included children's data or special category data personal data in some circumstances. I note that FB-I does not accept that the Breaches involved children's data or special category personal data.[40] However, my view, as outlined above, is that, in light of the nature of the processing concerned by the Facebook and Instagram services, this possibility cannot reasonably be excluded.

61. In general, therefore, in light of the matters outlined above, I consider, in agreement with the inquiry team's statement in the Final Inquiry Report, that the nature, scope, context and purposes of FB-I and Facebook, Inc.'s processing indicated that it was:

> *"expansive in nature, broadly-scoped, contextually extensive, and undertaken for wide-ranging purposes, the nature, scope, context, and purposes of the processing, along with the noted inherent risks of software bugs and vulnerabilities in the codebase, presented a significant risk to data subjects' rights and freedoms."*

62. I wish to note that FB-I does not accept that its processing presents such a risk.[41]

---

[37] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraph 1.2 and footnote 21, page 8. FB-I has explained that it defines a monthly active user of the Instagram service as a registered Instagram user who logged in and visited Instagram through the website or a mobile device in the last 30 days as of the date of measurement. As in relation to the Facebook service, this figure consists of active accounts rather than unique users.

[38] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 9.

[39] FB-I's Record of data processing activities (user data – EU region) (Section 5).

[40] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraphs 1.11 to 1.13, page 10.

[41] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraph 1.9, page 10.

Analysis of risks arising from personal data breaches such as the twelve Breaches the subject of the Inquiry

63. The types of physical, material or non-material damage which should be taken into account when assessing the risk to data subjects from personal data breaches are outlined in Recital 85 of the 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."*

64. 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.

65. The twelve Breaches which give rise to this Inquiry provide some examples of the types of risks to data subjects which can arise for assessment in connection with software bugs affecting the Facebook and Instagram services. In considering whether there has been an infringement of the GDPR and in assessing the risks presented by processing where relevant, I must avoid reasoning purely with the benefit of hindsight. For the avoidance of doubt, my assessment of the appropriateness of measures implemented by FB-I and my assessment of the related issue of the likelihood and severity of the risks is based on risks that were known or could reasonably have been identified or foreseen at the time under consideration. In that regard, I consider that the examples of the types of risks to data subjects in the twelve Breaches all ought to have been known to FB-I before the Breaches occurred.

66. I consider that the circumstances of each of the Breaches likely resulted, at a minimum, in a loss of control of personal data by the EU users affected (a form of "*physical, material or non-material damage*" which is expressly recognised by Recital 85 of the GDPR). In addition, certain of the Breaches could potentially have resulted in additional physical, material or non-material damage for EU users. This is usefully demonstrated by Breaches 1 and 10.

67. Breach 10 (which affected in excess of [redacted] EU users) is typical of a loss of control of personal data, and concerned a software bug related to the Facebook Photo API that led to additional photo types on Facebook which were not covered by user permissions being accessible by third-party apps. In addition to photos uploaded to the user's Timeline and photos the user was tagged in, this included:

> *"(i) photos contained in Stories (active and archived Stories), (ii) feedback reporting flow photos (when a user attaches an image to a bug they report); Marketplace photos (public photos of items for sale); (iii) temporary photos uploaded prior to their being published (stored temporarily to facilitate better posting reliability on Facebook); (iv) Facebook Groups (where the apps separately had permission to access groups photos)."*[42]

[42] Breach notification form for Breach 10 (22 November 2018) (Section 2.8).

68. Breach 1 (which affected up to [redacted] EU users) concerned a software bug which affected the blocking function on Facebook and Facebook Messenger for a period of time, with the result that during the time the bug was live, (i) a blocked user may have been able to see the posts of an impacted user if that post was Public, 'Friends of Friends,' or in a shared space like a Group or Page, and (ii) a previously blocked user of Facebook Messenger may have been able to message an affected user. As identified by the inquiry team in the Final Inquiry Report[43] (and recognised by FB-I), [44] there are multiple reasons why a user may wish to block another user on Facebook, including for reasons relating to "*harassment and bullying*". A failure in the blocking function resulted in a loss of control of personal data in that blocking actions taken by affected EU users to prevent others from seeing their posts or from communicating with them via Facebook Messenger were not given effect during the time that the software bug was operational. Further, certain EU users could have been exposed to additional non-material damage in the nature of upset or distress arising from unwanted communication, harassment or bullying behaviour by users they had attempted to block.

69. I wish to record that FB-I does not agree with the assessment of the Breaches in paragraph 66 above. In this regard, FB-I has submitted that:

> *"1.7 As noted at paragraph 57 of the PDD, Recital 85 GDPR 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" (emphasis added). The language of Recital 85 GDPR therefore suggests only that a data breach may result in physical, material or non-material damage if not addressed in a timely manner.*
>
> *1.8 As noted in Part A above, even if damage to EU Users was possible as a result of the Breaches, it did not occur, not least because all the Breaches were swiftly remedied. The software bugs were identified and remediated promptly, demonstrating the effectiveness of [FB-I]''s multi-layered technical and organisational measures. Furthermore, given that each of the software bugs had a limited scope, and often a limited duration, any risk of damage to EU Users resulting from them was limited."*[45]

70. However, for the reasons set out above, I am unable to accept FB-I's suggestion that no damage to EU users was possible, or that it can be definitively presumed that such damage did not in fact occur, because the twelve Breaches were quickly remedied. Although certain of the Breaches were remedied within a matter of hours, in other cases the underlying issues remained live for longer periods (for example, Breaches [redacted]). In connection with this, however, it is necessary to state that I recognise and have had due regard to the fact that at the time the twelve Breaches which are specifically the subject of this Inquiry were notified to the DPC, FB-I had assessed Breaches [redacted] as "*Medium Risk*", and Breaches [redacted] were each described by FB-I as "*Low Risk*". Further, FB-I has maintained in the Inquiry that overall it considers the risks to EU users from the twelve Breaches were "*limited*".[46] I also wish to acknowledge that it has not been possible, and nor is it the purpose of the Inquiry, to investigate how particular risks may have eventuated for specific EU users arising from the Breaches.

---

[43] Final Inquiry Report (2 December 2020), page 20.

[44] See Facebook, 'Letting People Know About a Blocking Bug' (2 July 2018) https://about.fb.com/news/2018/07/blocking-bug/.

[45] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraphs 1.7 to 1.8, page 9.

[46] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 6, 16, 18, and 20.

71. In summary, as I have previously stated, for the purpose of the analysis in this Decision, I agree with the view of the inquiry team in the Final Inquiry Report[47] that, in light of the inherent risk of software bugs occurring in the codebase underlying Facebook, Inc.'s systems which could result in personal data breaches within the meaning of Article 4(12) GDPR, as well as the nature, scope, context and purposes of the processing carried out by FB-I and Facebook, Inc. in connection with the Facebook and Instagram services, the processing for which FB-I was responsible as a controller, in general, presented a significant risk to the rights and freedoms of data subjects, and FB-I ought to have been aware of this risk at the time of processing. I have additionally taken into account that, although the twelve Breaches did involve risks to the rights and freedoms of data subjects and likely caused a degree of non-material damage for the EU users affected, it is not the purpose, nor would it be possible, for this Inquiry to investigate and establish how these risks may have materialised in individual cases during the time under consideration. I make the latter observation only to emphasise that the DPC has not been in a position to investigate the individual impact of the Breaches on the (upwards of) [redacted] specific EU users potentially concerned.[48]

State of the art and costs of implementation in the context of Article 32(1) GDPR

72. I have set out above certain considerations relating to the risks of the processing carried out for the purpose of providing the Facebook and Instagram services, taking into account its nature, scope, context and purposes, which are relevant to the analysis in particular in light of both Articles 24(1) and 32(1) and (2) GDPR. In addition to the matters outlined above, it is necessary, in the context of Article 32(1) GDPR, to have regard to state of the art and the costs of implementation of technical and organisational measures.

73. Guidance on the concept of the "*state of the art*" as referred to in the GDPR has been provided by the EDPB in its Guidelines 4/2019 on Article 25 Data Protection by Design and Default (20 October 2020). Although the guidelines are addressed to Article 25 GDPR, that provision contains similar concepts to Article 32 GDPR. In particular the EDPB guidelines indicate that the requirement to take into account the "*state of the art"* imposes an obligation for controllers, when determining the technical and organisational measures applicable to their processing, to take account of the current progress in technology on a continuous basis. The EDPB guidelines also recognise that:

> *"Existing and recognized frameworks, standards, certifications, codes of conduct, etc. in different fields may play a role in indicating the current "state of the art" within the given field of use. Where such standards exist and provide a high level of protection for the data subject in compliance with – or go beyond – legal requirements, controllers should take them into account in the design and implementation of data protection measures."*[49]

74. In the Final Inquiry Report, the inquiry team outlined their expectation that FB-I would have considered the state of the art in its implementation of appropriate technical and organisational security measures, including relevant best practice and published expert guidance made available by the European Union Agency for Cybersecurity (ENISA), National Institute for Standards and Technology (NIST), and International Organization for Standardization (ISO) (of which the inquiry team provided a series of examples).[50] Further, the inquiry team indicated their expectation that FB-I's measures would be analogous (rather than identical) to industry best practice as reflected by the

[47] Final Inquiry Report (2 December 2020), page 40.
[48] I consider this clarification necessary in light of FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part B, paragraph 1.10, page 10.
[49] Guidelines 4/2019 on Article 25 Data Protection by Design and Default (20 October 2020), page 8.
[50] Final Inquiry Report (2 December 2020), pages 40 to 43.

guidance, and that, whereas consulting and adhering to expert guidance represents one important means by which a controller can determine the appropriateness of its measures, the inquiry team was fully open to alternative approaches, provided sufficient reasoning informed the determination as to what measures were appropriate and why they were deemed appropriate.[51] I consider this to have been a proper approach to take in the circumstances.

Appropriate technical and organisational measures in the context of Article 5(1)(f), 5(2), 24 and 32 GDPR

75. In view of the above, and as discussed by the inquiry team in the Final Inquiry Report,[52] I consider that appropriate technical and organisational security measures taking account the state of the art in connection with FB-I and Facebook, Inc.'s processing would (in broad overview) involve, in accordance with Article 5(1)(f), Article 32(1), and in particular Article 32(1)(b) and (d) GDPR:[53]

    (1) ***A risk assessment framework*** directed to compliance with the GDPR, including (but not limited to) ongoing, regular and comprehensive risk assessments and reviews throughout the lifecycle of the processing, and a developed methodology for the calculation and recalculation of risk(s) associated with the processing that contributes to the ongoing implementation, maintenance, and improvement of technical and organisational measures.

    (2) ***Software vulnerability and bug management*** measures including (but not limited to) proactive, comprehensive, and robust documented policies and procedures, oversight of coding processes, adherence to established best practice, standards and guidance, experience-based methods, code reviews, threat simulations and layered manual and automated testing.

    (3) ***Incident response policies and procedures*** to ensure information security incidents and personal data breaches within the meaning of Article 4(12) GDPR are responded to in a timely and effective manner as they occur, including (but not limited to) measures to ensure that all incidents are handled in a consistent manner, definition of roles for each individual team involved in incident response and incident management, exercise of appropriate oversight over incident management, post-incident reviews and root-cause analysis.

76. In addition, I consider that, for the purpose of Article 5(2) and 24(1) GDPR, appropriate technical and organisational measures to enable FB-I to be able to demonstrate that processing is performed in accordance with the GDPR (including Article 32(1) and 5(1)(f) GDPR) would involve measures including (but not limited to) implementation of appropriate and effective data protection policies and incident management procedures in respect of information security incidents and personal data breaches within the meaning of Article 4(12) GDPR, processes to test and verify that internal policies and procedures are adhered to in practice, internal or external audits or reviews of FB-I and Facebook, Inc.'s implementation of appropriate technical and organisational security measures under the GDPR, and systems and procedures for maintaining appropriate documentation and records to enable FB-I and Facebook, Inc. to demonstrate the effectiveness of its technical and organisational measures and compliance with FB-I's obligations under the GDPR.

---

[51] Final Inquiry Report (2 December 2020), page 42.

[52] Final Inquiry Report, (2 December 2020), pages 43 to 50.

[53] In the Final Inquiry Report (2 December 2020), at page 43, the inquiry team also set out its expectations in relation to FB-I's adherence to the principles of confidentiality, availability and integrity under Article 32(1) and 32(1)(b) and (d) GDPR. I have integrated the inquiry team's observations in this regard with my analysis under the three main headings in the analysis which follows, where appropriate.

77. I wish to clarify that I do not agree that the above constitutes a "*rigid or prescriptive approach*" or "*specific obligations*" inappropriately formulated by the DPC in respect of the technical or organisational measures FB-I ought to have in place to ensure compliance with Articles 5(1)(f), 5(2), 24 and 32 GDPR.[54]

78. In addition, it is relevant to recall (as outlined previously at paragraph 29 above) that FB-I was specifically informed in the Appendix to the Commencement Notice that, where relevant supporting documentary evidence was requested in the queries, FB-I was being asked to provide:

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

79. I note, finally, that the cost of implementation is a factor to be taken into account when selecting appropriate technical and organisational measures in the context of Article 32(1) GDPR. In particular, the EDPB 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.[55]

Analysis relating to FB-I's compliance with Articles 5(1)(f), 5(2), 24 and 32 GDPR

80. As outlined previously, Articles 32(1) and 24(1) GDPR envisage that appropriate technical and organisational measures are to be determined and implemented by a controller taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and, in respect of Article 32(1), the state of the art and the costs of implementation. A number of relevant considerations in relation to each of those factors have been outlined above. The following section considers, in light of those considerations, whether in the period between 7 June 2018 and 4 December 2018, FB-I and Facebook, Inc. had implemented appropriate technical and organisational measures in light of Articles 5(1)(f), 5(2), 24 and 32 GDPR. Whereas, owing to the volume and agreed phasing of the submissions provided by FB-I in the Inquiry, the inquiry team adopted a chronological approach to its examination of the submissions, for the purpose of this Decision I have taken a holistic approach to the submissions, information and supporting documentary evidence provided by FB-I during the course of the Inquiry.

81. In assessing FB-I's compliance with the relevant provisions of the GDPR, I have considered the materials in the Inquiry which provide insight into the technical and organisational security measures that FB-I had in place at the time the twelve Breaches were notified between 7 June 2018 and 4 December 2018. For these purposes, I have not considered materials related to the Expert Review which concern changes or improvements FB-I made to its technical and organisational security measures following the commencement of the Inquiry (which are not relevant to the issue of FB-I's infringement of, or compliance with, the GDPR in the relevant period). Those measures which relate to changes or improvements which FB-I has made in the intervening period will be addressed, insofar as relevant, in the section of the Decision setting out my decision on corrective powers in accordance with Section 111(2) of the 2018 Act, below.

---

[54] I consider this clarification to be necessary in light of FB-I's Response to the Preliminary Draft Decision, Part C, paragraph 2.6, page 16.

[55] Guidelines 4/2019 on Article 25 Data Protection by Design and Default (20 October 2020), pages 8 to 9.

Risk assessment framework

82. As outlined previously, FB-I is the controller, within the meaning of Article 4(7) GDPR, of the personal data of EU users of Facebook and Instagram which is processed by Facebook, Inc., who acts as a processor under Article 4(8) GDPR on FB-I's behalf. Their relationship in this regard is governed by a data processing agreement (DTPA).[56] Facebook, Inc. is obliged under the DTPA to (inter alia) implement appropriate technical and organisational security measures as required by Article 32(1) GDPR.[57]

83. FB-I has outlined that it has a security team (made up of information security experts and engineers), which has input into Facebook's global Security, Policy, Access, Risk and Compliance ("SPARC") team. FB-I submits that the FB-I security team was therefore engaged directly in assessing risks and ongoing review and maintenance of the policies, procedures and processes that comprise the global information security framework applicable to the Facebook and Instagram Services.[58] FB-I has provided a list and copies of certain documentation (referred to further below) which is said to form part of the "*global security framework*" applicable to the Facebook and Instagram service, and outlined the FB-I security team's role in respect of each document by way of a RACI[59] table (indicating whether the FB-I security team was responsible, accountable, consulted, or informed in relation to each document).[60]

84. In relation to ongoing oversight over changes to the global security framework, FB-I has outlined that:

> *"Proposed changes to the global information security policies and procedures are reviewed and assessed for effectiveness regularly. Given the nature of the organisation, all policies and procedures are "living documents", which are continually updated in light of, and to reflect, learnings gained by experience, annually and as needed. Approved changes are communicated to senior management and the global security team through internal Facebook Groups. The security team (including representatives from the FB-I security team as appropriate) collaborates and communicates through weekly reviews of security-related incidents, including through several internal Facebook Groups (on various security topics, including product security and security by design) and in on-site and off-site trainings."*[61]

85. In relation to its engagement with the SPARC team's work on risk assessment and ongoing review of technical and organisational security measures, FB-I has indicated that:

---

[56] A copy of which was provided to the DPC with FB-I's Response to Queries 1 to 4 in the Commencement Notice (18 January 2019).

[57] FB-I's Response to Queries 1 to 4 in the Commencement Notice (18 January 2019), page 3.

[58] FB-I's Response to Queries 5 to 12 in the Commencement Notice for Breaches 5 and 6 (8 February 2019), pages 2 and 3.

[59] 'RACI' is a method of assigning responsibility for tasks or projects and is an acronym for '*responsible, accountable, consulted, informed*'.

[60] FB-I's Response to Queries 5 to 12 in the Commencement Notice for Breaches 5 and 6 (8 February 2019), pages 1 and 2. See explanation on page 2 "*FB-I is either (i) accountable (i.e., it owns the documents); (ii) responsible (i.e., leads the work to achieve the task, e.g. update); (iii) consulted (i.e., a member of SPARC in Dublin has been involved in the update process); or (iv) informed and able to input (i.e., a member of SPARC in Dublin has access to the documentation and the ability to provide input into its content*)."

[61] FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019), page 7.

> *"[…] the FB-I security team is engaged directly in the SPARC programme that regularly tests, assesses and evaluates the effectiveness of technical and organisational measures and updates such measures as necessary.*
>
> *The global SPARC team (which includes members of the FB-I security team) also evaluates security risk controls across the organisation, and coordinates and supports independent audits as they relate to security. SPARC works with cross-functional teams to ensure appropriate security policies and controls are in place and documented in the audit process. SPARC coordinates audits for PCI DSS compliance, SOC 2 assessments for various Facebook products, SOX compliance, and other compliance areas."*[62]

86. FB-I further stated in its submissions on the Preliminary Draft Decision that:

> *"As previously explained to the DPC in the Inquiry,* [redacted] *is used in order for [FB-I] to satisfy itself that [Facebook, Inc.'s] technical and organisational security measures are in place and operating effectively. Security measures are documented and tested by [Facebook, Inc.], and [FB-I] also performs periodic reviews of the controls testing program to validate that the technical and organisational measures in place that have been reviewed, documented and tested by [Facebook, Inc.] have been appropriately assessed as being effective. In such cases,* [redacted] *. [FB-I] can also, if needed,* [redacted] *. These steps enable [FB-I] to validate that technical and organisational measures have been implemented and are operating effectively, but it is not realistic – nor reasonable - to expect that such validation will have occurred at a granular level in relation to all specific aspects implicated in all personal data breaches notified to the DPC under Article 33 GDPR."*[63]

87. In response to queries by the DPC in the course of the Inquiry,[64] seeking relevant supporting documentary evidence demonstrating the engagement of FB-I's security team with the SPARC programme, FB-I provided three documents relating to the involvement of members of the FB-I security team in relevant risk assessments for H1 and H2 of 2018.[65]

88. FB-I has also indicated that "[i]n addition, the FB-I security team would also have been engaged by the FB-I data protection team on an ad-hoc basis in relation to incidents that were escalated to the FB-I data protection team by the process set out in the Data Incident Response Plan (DIRP)".[66]

89. As part of its Response to the Draft Inquiry Report (22 May 2020), FB-I also provided at Annex 2 a document entitled 'System and Organisation Controls (SOC) 2 Type II Report for Workplace @

---

[62] FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019), pages 7 and 8.
[63] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraph 2.9, page 17.
[64] Additional Queries (5 June 2019), Query 4.
[65] FB-I's Response to the Additional Queries (14 June 2019), page 4.
[66] See FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 38 to 39. A copy of the Data Incident Response Plan (25 May 2018) was provided to the DPC with FB-I's Response to Queries 5 to 12 in the Commencement Notice for Breaches 1 and 2 (26 January 2019).

Facebook for the period 1 January 2018 through 31 December 2018'.[67] This is a report[68] (reviewed by an independent auditor) describing security controls applied by Facebook, Inc. in respect of one of its products, Workplace Premium,[69] by reference to specific audit criteria.[70]

90. I have had regard to the information and submissions provided in the Inquiry with relevance to FB-I's frameworks for risk assessment and risk management, and, in particular, to the documents (including those referred to above) provided by FB-I by way of supporting documentary evidence which in my view are of particular relevance in this regard, as follows:

Document	Date	FB-I RACI
Security Partnership Team – Wiki	Undated	[redacted]
Security Policy Access Risk and Compliance - Wiki	Undated	
Information Security Policy Program - Wiki	Undated	
Gantt Chart Risk Assessments H2 2018	30/10/18	
Risk Assessment Resource Allocation 1	Undated	
Risk Assessment Resource Allocation 2	Undated	
Extract from GDPR InfoSec Narrative (WIP)	Undated	
Policy Development Operations – Summary of Policy Development Lifecycle - Wiki	Undated	
Infosec Policy Pipeline – Wiki	Undated	
System and Organisation Controls (SOC) Type II Report for Workplace @ Facebook for the period 1 January 2018 through 31 December 2018	14/08/19	-

91. As appears from the above, several of the documents are in the form of internal 'Wiki' documents from Facebook's intranet which provide high level summaries in the style of information sheets targeted at employees on the policies and activities to which they relate. I do not criticise the specific format or content of those documents, as I appreciate that each controller and processor is different in its organisational approach to implementing appropriate technical and organisational security measures, and it would not be appropriate for the DPC to take a rigid or prescriptive approach to the internal procedures or policies organisations have in place to ensure compliance with their security and accountability obligations under the GDPR. However, whereas I acknowledge that the internal 'Wiki' documents referred to above provide basic information in relation to a "*global security framework*" place at FB-I and Facebook, Inc. which reflects aspects of an approach to technical and organisational security taking into account the state of the art, I do not consider that such documents, in and of themselves, tend to demonstrate FB-I's compliance with its security and accountability obligations under the GDPR in practice for the purposes of this Inquiry, whether in the context of each of the twelve Breaches, or more generally. In its submissions in response to the

[67] FB-I's Response to the Draft Inquiry Report (22 May 2019), page 53 and Annex 2.

[68] The American Institute of Chartered Public Accountants (AIPCA) outlines that SOC 2 examinations concern "*controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems*". See AIPCA, 'SOC 2® - SOC for Service Organizations: Trust Services Criteria' <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html>

[69] Facebook's Workplace product is an enterprise connectivity platform (available in Standard and Premium versions) which allows enterprises to establish and manage an internal Facebook community for its employees.

[70] In particular, the American Institute of Certified Public Accountants' (AICPA) 'Trust Services Principles', TSP Section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

Preliminary Draft Decision, FB-I disagreed with the analysis in this paragraph, on the basis that *"[w]hen viewed as part of an overall compliance structure, [the internal 'Wiki' documents] do demonstrate compliance with [FB-I]'s accountability obligations - and no adequate reasoning has been provided by the DPC to support a conclusion to the contrary*."[71] In this regard, I wish to reiterate that the reason for my view is that the high level overviews of the activities described in the internal 'Wiki' were not sufficient, without more, to enable a supervisory authority to review and/or validate the operation of the technical and organisational measures to which they relate.

92. Likewise, the document entitled 'Extract from GDPR Infosec Narrative (WIP)' appears to be an extract from a draft document summarising the various technical and organisational security measures in place at Facebook, Inc., but I do not consider that such a summary can be considered to demonstrate such measures in real terms.

93. The document entitled 'Gantt Chart Risk Assessments H2 2018' is a status update for an internal Facebook group 'InfoSec Risk Assessments Programme' dated 30 October 2018, which shows an image of a PDF containing a Gantt chart[72] showing the timeline for risk assessments planned to be completed in H2 2018. The status update states, for example, that risk assessments for [redacted] were on track to be completed by mid-to-end January 2019. This document evidences the existence of a programme in place at Facebook, Inc. for conducting risk assessments relating to various Facebook products and services in 2018 and early 2019. However, the DPC has not, for example, been provided with supporting documentary evidence which provides insight into any actual risk assessments which may have been conducted in respect of the products and services involved in the twelve Breaches the subject of this Inquiry (for example, documents generated by relevant teams within FB-I or Facebook, Inc. which record the scope, methodology, conclusions, recommendations or other outputs of such risk assessments). The documents entitled 'Risk Assessment Resource Allocation 1' and 'Risk Assessment Resource Allocation 2' (together with the Gantt chart previously described) show that members of FB-I's security team were involved in risk assessments conducted by Facebook, Inc. for H2 2018 (and in some instances were risk assessment team leads), but provide no further insight into FB-I's activities in this field. I consider it important, at this point, to address the following submission made by FB-I:

> *"2.14 [FB-I] also notes the DPC's finding in the PDD that it had not been provided with "any supporting documentary evidence which provides insight into any actual risk assessments which may have been conducted in respect of the products and services involved in the [Breaches]."*
>
> *2.15 While it is not entirely clear to [FB-I] precisely what the DPC expects in relation to risk assessments "in respect of the products and services involved" in relation to specific breaches, it is not feasible to review every possible interaction of every possible software permutation for every product such that a relevant risk assessment could be produced on such a granular basis in relation to each breach that might occur. In this regard, [FB-I] notes that the GDPR requires appropriate technical and organisational security measures, utilising a proportionate, risk-based approach (which is constantly evolving). [FB-I] is not required – and cannot reasonably be required - to perform (and therefore demonstrate) risk assessments on such a granular level as appears to be suggested by the DPC in*

[71] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraphs 2.7 to 2.8, pages 16 to 17.
[72] A type of bar chart showing the progress of tasks in a project against a time schedule.

the PDD. Such an approach would be inconsistent with the fundamental principles of GDPR and would be impossible to comply with in practice."[73]

94. To be clear, the DPC has not, at any point in the Inquiry (whether expressly or by implication), stated the expectation that FB-I ought to "*review every possible interaction of every possible software permutation of every product such that a relevant risk assessment could be produced on […] a granular basis".* The observation in the previous paragraph is simply that, whereas the documents entitled 'Gantt Chart Risk Assessments H2 2018', 'Risk Assessment Resource Allocation 1' and 'Risk Assessment Resource Allocation 2' appear to indicate that in or around H2 2018 certain risk assessments were scheduled (for example, for [redacted]), the DPC was not provided with any further information regarding how such risk assessments were conducted or the outcomes of same, or any other risk assessments which may have carried out relating to other Facebook or Instagram products or features concerned by the Breaches. For that reason, the documents entitled 'Gantt Chart Risk Assessments H2 2018', 'Risk Assessment Resource Allocation 1' and 'Risk Assessment Resource Allocation 2' were limited in what they tended to demonstrate to the DPC about FB-I's compliance with the relevant provisions of the GDPR in the context of the Breaches examined.

95. The document entitled 'System and Organisation Controls (SOC) 2 Type II Report for Workplace @ Facebook for the period 1 January 2018 through 31 December 2018' is specific to Facebook's Workplace Premium product, and its scope is expressly stated to be limited to that particular product.[74] Limited references to Facebook's Workplace product were made in the Inquiry in connection with Breach [redacted][76]

96. In the Inquiry, FB-I stated that it was providing the SOC 2 Type II report for Workplace Premium for 2018 to the DPC "in order to assuage any concerns of the Inquiry Team regarding the implementation of such measures […] by way of verification of the information and the evidence FB-I has already provided in the Inquiry. These assessments are carried out for certain Facebook products used by businesses (in this case, Workplace), but they cover the product security, software development and vulnerability management controls that apply across all of Facebook's infrastructure."[77]

---

[73] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraphs 2.14 to 2.15, page 18.

[74] See in particular '*Section III – Description of the Workplace Premium by Facebook Product relevant to Security, Availability, and Confidentiality'* at page 12: "*This section of the report was prepared by the management of Facebook […] and is intended to provide user organisations with information about the Workplace Premium by Facebook Product's relevant internal controls […] It does not and is not intended to encompass all aspects of the services or procedures performed by Facebook, Inc.*" Similarly, *'Section II – Independent Service Auditor's Assurance Report*' is expressed to be limited to the controls in the description provided by Facebook, Inc. in the report, and, further, specifically excludes the information provided in *'Section V – Workplace Premium by Facebook and General Data Protection Regulation (GDPR), Security Notifications and Data at Rest'*.

[75] Response to Queries 5 to 12 in the Commencement Notice for [redacted] page 3.

[76] FB-I's Response to Queries 5 to 12 in the Commencement Notice for [redacted]), page 4.

[77] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 53.

97. I have taken into account FB-I's submissions as to the relevance and content of the SOC 2 Type II report,[78] but ultimately I agree with the inquiry team's analysis in the Final Inquiry Report as to its relevance.[79] While the examination in the report is limited to the Facebook Workplace Premium product, I recognise that the SOC 2 Type II report contains descriptions of certain technical and organisational security measures which may apply more generally across the Facebook service, as well as recording testing performed by an independent auditor to verify that such measures were implemented as described by reference to the specific audit criteria used. Audits by independent third parties can constitute valuable processes for risk assessment and review of a controller's implementation of risk management measures. However, it is nonetheless relevant to observe that the SOC 2 Type II report: (i) does not address controls applicable to the Instagram service, which was involved in five of the Breaches, and its associated risks, (ii) is expressly not intended to cover Facebook products other than Workplace Premium, and as such is not evaluative of the wider range of Facebook products which were concerned by seven of Breaches and their associated risks, (iii) does not examine controls in place at FB-I as the controller of personal data of EU users of the Facebook and Instagram services, and (iv) I note that Section V, entitled 'Workplace Premium by Facebook and the General Data Protection Regulation (GDPR), Security Notifications and Securing Data at Rest' is specifically excluded from the scope of the independent auditor's review. I do not consider that FB-I's submissions on the Preliminary Draft Decision in respect of this issue support an alternative view.[80]

98. Although FB-I's submissions and the documents listed above outline aspects of the implementation of procedures for risk assessment and review of risk management measures by FB-I in respect of the processing of EU users carried out on its behalf by Facebook, Inc., I am not satisfied that FB-I has provided sufficient information and supporting documentary evidence in the Inquiry to demonstrate compliance with its obligations in this regard under the GDPR.

Software vulnerability and bug management

99. As outlined previously above, FB-I has submitted that software bugs are an inherent risk, and that "the larger the codebase, the more potential exists for unanticipated interactions of code that can cause unintended software behaviours."[81] FB-I submits that:

> *"[Facebook, Inc.] caught thousands of vulnerabilities at different stages of the software development lifecycle […] through the various layers of product security controls it has in place. [Facebook, Inc.] prevented many more, through the secure application frameworks it maintains, which work to prevent various classes of vulnerabilities from ever being introduced into the code in the first place.*
>
> *The 12 software bugs at issue therefore represent a very small subset of these bugs, which are widely accepted to be an inherent risk, that were only detected after they caused an unintentional exposure or deletion of user data. [FB-I] submits that the fact that there were relatively few such bugs shows that*

[78] Including the submissions in FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 58 and 59 and footnote 55.
[79] Final Inquiry Report (2 December 2020), pages 102 to 104.
[80] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraph 2.11, pages 17 to 18. I note that this paragraph repeats, substantially, the submissions previously made in FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 53, 58 and 59, and footnote 55.
[81] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 5.

[Facebook, Inc.'s] product security controls (which are overseen by [FB-I]) are effective overall, particularly in the relevant context."[82]

100. FB-I maintains that it deploys a 'defence-in-depth' approach by maintaining multiple layers of controls designed to detect software bugs in different ways at different points of the software development lifecycle.[83]

101. I have had regard to the full extent of FB-I's submissions in which it describes a range of technical and organisational security measures relevant to software vulnerability and bug management.[84] In FB-I's Response to the Draft Inquiry Report (22 May 2020), the measures are broadly summarised under the following headings, and include:[85]

(1) ***Secure application frameworks***, which FB-I describes as programming language extensions and and libraries of common bits of code that provide Facebook, Inc. engineers with built-in safeguards against various known types of vulnerabilities and coding flaws as they write code. It is stated engineers receive training during their on-boarding on how to use the secure application frameworks.

(2) ***Automated testing tools***, referring to analysis tools that scan for known types of problematic code patterns, including static analysis tools, which review written source code itself, and dynamic analysis tools, which run the code to observe errors as the programme is running. In particular, FB-I has described the operation of Facebook, Inc.'s Zoncolan tool, a static analysis tool which automatically examines Facebook, Inc.'s codebase.

(3) ***Peer reviews***, referring to a system of mandatory manual review of code changes prior to their release by an engineer other than the engineer who is the author of the change. The reviewing engineer can, if they identify any issues in the code, reject the change and refer it back to the original engineer for amendment.

(4) ***Design reviews***, whereby Facebook, Inc.'s ProdSec team has the opportunity to view all ongoing and upcoming projects and to proactively select projects for security review based on a defined set of strategic risk priorities. FB-I has stated that the ProdSec team conducts numerous such reviews each year.

(5) ***Phased deployment and testing***, which involves Facebook, Inc. deploying new code first to an internal version of the Facebook and Instagram services, available to employees only, before being deployed to the public more broadly. It is outlined that this provides an opportunity for functionality issues to be identified internally (a process known as 'dogfooding'). The code change may then be rolled out on a phased basis via a piece of functionality known as Gatekeeper which allows a code change to be tested on a particular segment of users (e.g., to

---

[82] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 11.

[83] FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 14 to 16 and 39. FB-I refers in this regard to a Facebook News blogpost, Collin Greene, "Designing Security for Billions," Facebook, (25 January 2019), available at https://newsroom.fb.com/news/2019/01/designing-security-for-billions/.

[84] In particular, FB-I's submissions directed to this matter summarised in the breach notification forms, FB-I's Response to Queries 5 to 12 in the Commencement Notice for Breaches 5 and 6 (8 February 2019), pages 1 and 2 and Annex, FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019), pages 6 to 11, FB-I's Response to Additional Queries (14 June 2019), FB-I's letter to the DPC dated 30 August 2019 concerning the principal issues in the Inquiry, and FB-I's Response to the Draft Inquiry Report (22 May 2020).

[85] FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 39 to 45.

10% of users from a certain geographic area, with all other users either seeing the old version of the feature or no version of the feature).

(6) ***Penetration testing and vulnerability scanning***, referring to Red Team exercises (threat modelling exercises to assess how security systems respond to staged attacks), use of manual and automated penetration testing techniques to identify gaps in security controls, and use of automated scanning tools and manual scanning for vulnerabilities by Facebook, Inc.'s vulnerability management team, which collects information about known and newly identified security vulnerabilities from third party sources (such as the Common Vulnerabilities and Exposures Database[86] and the National Vulnerability Database[87]).

(7) ***A bug bounty programme***, by which external security researchers are incentivised to report software bugs they find or observe in relation to the Facebook and Instagram services (it is referred to also throughout the responses as Facebook, Inc.'s 'white hat' programme).[88]

102. I have taken due account of the detailed information FB-I has provided as to the effectiveness of its layered approach to security, including several specific examples referred to in FB-I's Response to the Draft Inquiry Report (22 May 2020). [89]

103. In addition, I have examined the information and documentation supplied by FB-I in the Inquiry by way of supporting documentary evidence with relevance to the technical and organisational security measures FB-I and Facebook, Inc. had in place at the relevant time relating to software vulnerability and bug management. The documents which I consider to be particularly relevant to this matter are the following:

Document	Date	FB-I RACI
Detection and Security Infrastructure - Wiki	Undated	[redacted]
Product Security - Wiki	Undated	
Product Security Assessment and Analysis - Wiki	Undated	
Data Security Systems - Wiki	Undated	
Integrity Infrastructures - Wiki	Undated	
Internal Detection Engineering - Wiki	Undated	
Red Teams - Wiki	Undated	
Whitehat Information	29/11/18	
Coding at Facebook - Wiki	Undated	
The Code Review Process - Wiki	Undated	
Diffs Best Practice - Wiki	Undated	

[86] Common Vulnerabilities and Exposures Database (CVE) maintained by The Mitre Corporation and sponsored by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), see https://cve.mitre.org/.

[87] National Vulnerability Database (NVD) maintained by the U.S. National Institute of Standards and Technology, see https://nvd.nist.gov/.

[88] I note that in the chronologies FB-I has provided in the Inquiry, FB-I has stated that the software bugs giving rise to [redacted] were [redacted]. Otherwise, several of the Breaches, including [redacted] It is indicated that [redacted] was [redacted]

[89] FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 40 and 43.

Security Oncall Information	Undated	[redacted]
Security n00bs Portal - Wiki	Undated	
Privacy and Security Awareness Training - Wiki	Undated	
User Data Access Training Information	Undated	
Bootcamp Training Slides – Ethics and Privacy	Undated	
System and Organisation Controls (SOC) Type II Report for Workplace @ Facebook for the period 1 January 2018 through 31 December 2018	14/08/19	-

104. Having considered all of the above information, I recognise that the technical and organisational security measures described by FB-I are indicative of an approach to software vulnerability and bug management containing features which may be considered analogous to industry best practice and the state of the art, and, if sufficiently demonstrated, would, in principle, be capable of satisfying the requirement to ensure a level of security appropriate to the risk involved in FB-I and Facebook, Inc.'s processing. However, I do not consider that sufficient information has been provided in FB-I's responses to the Inquiry to effectively demonstrate the implementation of the wide range of technical and organisational security measures described in accordance with FB-I's accountability obligations.

105. In particular, having carefully reviewed the documents at paragraph 103 above, I consider that, although those documents summarise certain of the measures referred to by FB-I general terms and illustrate aspects of a "*global security framework*", including secure coding practices FB-I and Facebook, Inc. state were in effect at the relevant time, I do not consider that the documents may be taken as evidencing FB-I's compliance with its security and accountability obligations under the GDPR, in terms of Facebook, Inc.'s and FB-I's actual adherence to those procedures in practice by reference to the underlying facts of the twelve Breaches. Whereas the documents referred to in paragraph 103 above outline elements of the software vulnerability and bug management measures described in FB-I's submissions, they do not constitute records documenting the actual carrying out of the activities in practice in the context of the twelve Breaches. In this regard, where FB-I (in its Response to the Draft Inquiry Report (22 May 2020), pages 72 to 84) argues that it has "*evidenced the implementation of [appropriate technical and organisational] measures in relation to each of the Breaches during the course of the Inquiry*", in effect, FB-I's submissions at this point go no further than stating that, in general, the descriptive or narrative information FB-I provided to the DPC in the breach notification forms and the chronologies of the twelve Breaches in the Inquiry[90] relating to how the Breaches were discovered, investigated and remediated, is consistent with various elements of the policies and procedures forming part of the "*global security framework*". What is lacking, however, is supporting contemporaneous documentation or records created during the management of the underlying code changes or handling of the twelve Breaches which provide insight into the actions taken by Facebook, Inc. and FB-I at the relevant time and which substantiate the information provided to the inquiry team in the breach notification forms and the information provided by FB-I during the course of the Inquiry.

106. By way of example, in respect of [redacted] FB-I stated:[91]

> *"(b) As explained in [FB-I]'S Replies dated [redacted] […]:*
>
> *(i) "[redacted]*

[90] For example, in FB-I's Responses to Queries 5 to 12 in the Commencement Notice for the twelve Breaches.
[91] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 72.

> [redacted]*." The [InfoSec Incident Response Policy] and the [Data Incident Response Plan] make clear that incidents reported from various internal (such as dogfooding) and external channels (such as Workplace, Facebook Feedback Groups and white hat) are investigated by [Facebook, Inc.] engineers* [redacted]

107. Similarly, for example, in respect of [redacted] FB-I stated: [92]

> *"(c) As explained at section 8 of the [breach notification form], and in more detail in [FB-I]'s Replies dated* [redacted] *[…]: "As soon as the issue was discovered -* [redacted]*. The incident has now been fully resolved." <u>This was in accordance with The [InfoSec Incident Response Policy] and the [Data Incident Response Plan]</u>."*

108. As will be clear from my observations, above, I do not agree with FB-I that that such examples show that "the information and documentation FB-I provided in the Inquiry demonstrate that various relevant technical and organisational measures were implemented" in relation to the twelve Breaches. A statement that steps were taken or activities were performed in accordance with a policy or procedure, in the absence of documentation or records evidencing the steps or activities actually implemented, is not sufficient to meet the obligation to demonstrate that processing is carried out in compliance with the GDPR, as required by the accountability principle set out in Article 5(2) and 24(1) GDPR.

109. I have also taken note of the documentation relating to data privacy training provided to Facebook, Inc. and FB-I's employees which I consider to be a positive measure. However, the training provided is of a general nature and predominantly directed to employee access and use of user data, as opposed to training directed to preventing and responding to software vulnerabilities and incidents such as those giving rise to the twelve Breaches in this Inquiry. I note, in addition, that the training documentation does not at appear to be targeted specifically towards compliance with the GDPR.

110. Further, I have outlined, at paragraph 97 above, the reasons for my view that the document entitled 'System and Organisation Controls (SOC) 2 Type II Report for Workplace @ Facebook for the period 1 January 2018 through 31 December 2018' does not sufficiently demonstrate the implementation of the security measures relied on by FB-I in the Inquiry in respect of the Facebook and Instagram services, and those reasons are equally applicable in this context.[93] In addition, FB-I, in its submissions in the Inquiry, has outlined in some detail the activities of teams such as (for example) the ProdSec team within Facebook, Inc. in detecting and mitigating software vulnerabilities, but does not provide supporting documentary evidence to substantiate the information provided.

111. I wish to note, in addition, that I disagree with FB-I's submission that it should not have to provide relevant supporting documentary evidence of, for example, secure application frameworks or automated testing tools (such as its Zoncolan tool) which operate generally and routinely at Facebook, Inc. to prevent software vulnerabilities.[94] Records of documentation such as technical

[92] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 74.
[93] As set out above, I have taken account of FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraph 2.23, page 20, but my assessment on this point has not changed.
[94] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 53.

standards or specifications adhered to by such measures, updates, reviews, audits or testing performed on them, and logs or reports generated during their routine operation, constitute just some possible examples of the type of documentation which controllers might be expected to supply in this regard. The fact that a particular technical or organisational security measure operates "*generally*" or "*routinely"* does not mean that it is unnecessary to maintain appropriate records in respect of it in light of Article 5(2) and Article 24 GDPR.

112. In its submissions on the Preliminary Draft Decision, FB-I has asserted generally, by reference to the technical and organisational security measures summarised at paragraph 101 above (namely FB-I's secure application frameworks, automated testing tools, peer reviews, design reviews, phased deployment and testing, penetration testing and vulnerability scanning, and bug bounty programme), that often it will be impossible to demonstrate the implementation of such measures in the context of a specific personal data breach within the meaning of Article 4(12) GDPR.[95] FB-I has maintained in its submissions on the Preliminary Draft Decision, as in the Inquiry, that such measures are implemented "*programmatically*" by Facebook, Inc., but could not have been usefully or reasonably demonstrated to the DPC in the specific context of the Breaches at issue in this Inquiry. As outlined above, I do not consider that response takes appropriate account of FB-I's obligations under Articles 5(2) and 24 GDPR to be able to demonstrate the effective and appropriate technical and organisational security measures that FB-I and Facebook, Inc. have implemented in order to comply with Articles 5(1)(f) and 32 GDPR. As set out above, I consider that it is not sufficient for FB-I to rely on, or for the DPC to accept, the narrative descriptions in FB-I's submissions of the complex security framework in place at Facebook, Inc., in the absence of appropriate documentation or records such as would enable the DPC to objectively review or verify the effective implementation of the technical and organisational security measures described.

Incident response and management policies and procedures

113. FB-I has outlined that, in accordance with Articles 32(1)(d) and 28(3)(f) GDPR, the DTPA between Facebook, Inc. and FB-I requires Facebook, Inc. to assist FB-I with its obligations pursuant to Articles 32 to 36 of the GDPR.[96] The defined process for handling and responding to information security incidents (including personal data breaches) is described in a series of documents including the InfoSec Incident Handling Standard, the InfoSec Incident Response Policy and the Incident Response Roles, the Data Incident Response Plan and the Legal IRP Flow Overview.

114. In response to a query by the DPC,[97] FB-I outlined that:

> *"The InfoSec Incident Response Policy is intended to be an overarching framework policy with each individual team involved in responding to information security incidents developing their own incident response policies and processes. As explained in the InfoSec Incident Response Policy, it is intended to "define the scope, roles, responsibilities, and minimum baselines for performing information security incident response activities". The InfoSec Incident Handling Standard is intended to provide further details, and sets out some of the teams responsible for responding to various types of information security incidents. As stated in the InfoSec Incident Handling Standard, Privacy*

[95] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraphs 2.24 to 2.27, pages 20 to 23.
[96] FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019), page 8.
[97] Additional Queries (5 June 2019), Query 2.

Legal (including the FB-I data protection legal team) are one of those teams. The DIRP sets out the Privacy Legal team's incident response processes.

The various policies interact and complement each other in a number of ways. For example, the InfoSec Incident Handling Standard makes clear that Privacy Legal (which includes FB-I's data protection legal team) must be notified "when an information security incident involving personal data is identified" and that they are then "responsible for escalating a personal data incident in adherence to" the DIRP.

FB-I is continually looking at ways to improve its written policies and, in light of FB-I's recent experiences and learnings, it has become apparent that the various incident response policies in place within FB-I (and [Facebook, Inc.]) could benefit from further refinement so they interact more effectively and more accurately reflect the actual practices and processes which have been developing since 25 May 2018."[98]

115. I have taken into account the information and submissions provided in the Inquiry with relevance to FB-I's procedures for information security incident management, and, in particular, to the documents (including those referred to above) provided by FB-I by way of supporting documentary evidence which, in my view, are of particular relevance in this regard, as follows:

Document	Date	FB-I RACI
Data Incident Response Plan	25/05/18	[redacted]
Legal IRP Flow Overview	Undated	
Infosec Handling Standard – Wiki	Undated	
Infosec Incident Response Policy – Wiki	Undated	
Incident Response Roles – Wiki	Undated	
IMOC Cheat Sheet – Wiki	Undated	
Infosec Incident Handling Standard History	Undated	
Infosec Incident Response Policy History	Undated	

116. The Data Incident Response Plan furnished by FB-I in the Inquiry sets out a procedure for teams within Facebook, Inc. to refer information security incidents involving personal data to Facebook, Inc.'s Privacy Legal team (and, where applicable, FB-I's EU Data Protection Legal Team). FB-I has also provided a document entitled Legal IRP Flow Overview which is said to supplement the other incident response documents provided to the DPC in the Inquiry and summarises the procedures followed by FB-I and Facebook, Inc. since around mid-July 2018 in relation personal data incidents,[99] and includes definition of roles for FB-I's EU data protection legal team in relation to assessment and notification to regulators of personal data incidents affecting data subjects for which FB-I is a controller.

117. The document entitled 'InfoSec Incident Response Policy' states that its purpose is to "define the scope, roles, responsibilities, and minimum baselines for performing information security incident response activities" within Facebook, Inc. More specific details of the roles and responsibilities of the various teams in Facebook, Inc. involved in information security incidents (referred to in the documentation as 'site events' i.e. SEVs) are set out in the 'InfoSec Incident Handling Standard'. The document entitled 'Incident Response Roles' is a glossary of important roles referred to in the

[98] FB-I's Response to the Additional Queries (14 June 2019), pages 2 and 3.

[99] A copy of the Legal IRP Flow Overview was provided to the DPC with FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019) and is described at page 8 of same.

previous documents, and the 'IMOC Cheat Sheet' is a set of instructions for Incident Manager On Call (IMOC) (the person with responsibility for carrying out the incident response process in relation to a SEV).

118. Having in place policies and procedures such as the InfoSec Incident Response Policy, Infosec Incident Handling Standard, DIRP and the Legal IRP Flow overview can constitute an appropriate organisational measure to assist the assessment and mitigation of security risks to data subjects arising from personal data breaches as defined in Article 4(12) GDPR. However, it is difficult to assess the effectiveness of these procedures in the period between 7 June 2018 and 4 December 2018 in the absence of documentation evidencing the manner in which they were implemented in practice in the context of any of the twelve Breaches the subject of this Inquiry. For example, in Query 5 in the Commencement Notice, FB-I was asked to provide a full chronology of events which occurred immediately after each of the twelve Breaches, to include "*relevant supporting documentary evidence including, but not limited to copies of emails, minutes of meetings, supporting policies and procedures*". FB-I has provided chronologies of the Breaches and relevant policies and procedures in connection with Queries 5 to 12 in the Commencement Notice in connection with each Breach, but has not included additional supporting documentary evidence that would tend to demonstrate how each of the policies and procedures outlined operated in real terms in their application to any of the twelve Breaches in the Inquiry.

119. This is particularly relevant given FB-I's submission that the InfoSec Incident Response Policy "is intended to be an overarching framework policy with each individual team involved in responding to information security incidents developing their own incident response policies and processes".[100] As observed by the inquiry team,[101] although FB-I's incident management measures required that several individual teams designated as responsible for incident response should derive their own distinct incident handling procedures from the overarching framework policy, the only examples provided to the DPC were the DIRP and the Legal IRP Flow Overview, applicable to Facebook, Inc.'s Privacy Legal team and applicable FB-I's EU Data Protection Legal Team. I note, in addition, that, while the Legal IRP Flow Overview and the DIRP are geared specifically towards compliance with the GDPR, other documents such as the InfoSec Incident Response Policy and the InfoSec Incident Handling Standard are more general and tend not to refer to data protection law obligations under the GDPR in any detail.

120. Further, it is not entirely clear, from the chronologies of the twelve Breaches provided by FB-I, which procedures were applied, and how they were applied, by the different teams involved at Facebook, Inc. and FB-I. By way of example, only the chronologies for [redacted] and [redacted] refer to the involvement of an Incident Manager On Call (IMOC), but, without the necessary context to explain why (or in the context of which incident response procedure) this occurred. The chronologies for (by way of example) [redacted] refer to [redacted]" investigating the incident, but do not indicate [redacted], or what incident response procedure was followed, although several teams are named in the InfoSec Incident Response Policy, the InfoSec Incident Handling Standards, and the DIRP. Further, from the chronologies for each of the twelve Breaches, it is not clear whether or to what extent the DIRP was implemented by Facebook, Inc. and FB-I, or, for example, whether a Privacy Legal Intake Form was completed by the detection teams within Facebook, Inc., documenting the facts to make a notification decision and the analysis that justified the decision, or whether and to what extent

[100] FB-I's Response to the Additional Queries (14 June 2019), pages 2 and 3.
[101] Final Inquiry Report (2 December 2020), pages 84 to 85 and 113.

Privacy Legal or FB-I's EU Data Protection Legal team [redacted] in accordance with the DIRP.

121. In addition, it appears, from a reading of the DIRP, the InfoSec Incident Response Policy, and the InfoSec Incident Handling Standard, that, if the policies and procedures set out in each of them were implemented as envisaged, the relevant roles and teams within Facebook, Inc. and FB-I would have generated a substantial volume of documentation and records in the context of each of the twelve Breaches. In this connection, the inquiry team noted in the Final Inquiry Report[102] that the DIRP envisions that "*activities from detection to mitigation (end-to-end) should be documented*" including, inter alia, completion of a Privacy Legal Intake Form by the relevant detection teams and provision of that form to the Privacy Legal team. It is further indicated in the DIRP that detection teams are required to document matters relating to personal data breaches in locations relevant to them and that Privacy Legal are required to "*maintain the source of truth document when addressing a personal data incident*", and keep a 'Personal Data Incident Register'. Further, the InfoSec Incident Response Policy envisions that "*[b]asic details must be captured for all detected or reported information security incidents*" and that "*[e]vidence relating to information security incidents should be collected for the purposes of permitting root cause analysis where required, and resultant regulatory or legal action. This evidence should be gathered, recorded, and maintained in a form that will withstand internal and external scrutiny (i.e., evidence should be admissible, sufficient, and unaltered)*". Likewise, the InfoSec Incident Handling Standard requires, *inter alia*, that a "*minimum amount of data*", will be captured where information security incidents occur.[103]

122. In response to a query by the DPC in the Inquiry,[104] requesting FB-I to provide the "*minimum amount of data*" captured in respect of each of the twelve Breaches, as required by the InfoSec Incident Handling Standard, FB-I replied that:

> *"As the DPC will hopefully appreciate, the incident details referred to inevitably change over the course of an information security incident (for example, many of the details referred to constantly evolve as an incident is investigated). The InfoSec Incident Handling Standard states that this is the minimum information that must be captured in the course of handling incidents, it does not require it to be captured in this form nor does it contemplate a set of records in the form of the table. As such, the information is captured in a variety of mediums and documents and updated in the course of the incident response life-cycle. As such, it is not clear, therefore, what information FB-I can usefully provide to the DPC in response to Question 8 (particularly in circumstances where FB-I has provided the DPC with detailed chronologies and information in relation to each of the Data Breaches in relation to the Inquiry). In the event that there is particular additional information that the DPC requires in addition to the chronologies, please let us know and FB-I will endeavour to provide it."*[105]

123. The absence of supporting documentary evidence which demonstrates how each of the relevant incident response policies and procedures were applied to any of the twelve Breaches in the Inquiry means that I am not in a position to verify that they were applied consistently and adhered to

[102] Final Inquiry Report (2 December 2020), page 61.

[103] Specifically, a set of incident details including the title, owner/POC, description, SEV level, incident impact, incident status, start time, and restoration time estimate, set out in the form of a table at page 4 of the InfoSec Incident Handling Standard.

[104] Additional Queries (5 June 2019), Query 8.

[105] FB-I's Response to the Additional Queries (14 June 2019), pages 6 and 7.

effectively at the relevant time. Further, I consider that FB-I's inability to provide the DPC with the supporting documentary evidence that, for example, was apparently required by the InfoSec Incident Response policy to be "*collected for the purposes of permitting root cause analysis where required, and resultant regulatory or legal action*" is indicative that FB-I and Facebook, Inc. did not have the appropriate systems in place to ensure the necessary documentation of information security incidents (and personal data breaches within the meaning of Article 4(12) GDPR) to meet its security and accountability obligations under the GDPR. Even where "*information is captured in a variety of mediums and documents and updated in the course of the incident response life-cycle*", it is necessary to have a workable system in place to ensure that incident response measures are documented in a manner that enables a supervisory authority to review a controller's compliance with the GDPR.

124. FB-I has confirmed that "[a]fter the incidents that led to the Data Breaches […] were resolved, they have been considered further in a periodic incident management review process. This process aims to identify trends and lessons to be learned in order to try to prevent similar incidents from recurring."[106] FB-I further provided a list of dates of "regular scheduled review meetings" in late 2018 and early 2019 in which each of the twelve Breaches individually were subject to post-incident review,[107] and has summarised examples of actions taken on foot of the reviews as follows:

> *"(a) In relation to* [redacted] *a number of additional steps were taken in relation to* [redacted].
>
> *(b) In relation to* [redacted] *[Facebook, Inc.'s] engineers* [redacted].
>
> *(c) In relation to* [redacted] *a number of changes to [Facebook Inc.'s]* [redacted] *were made.*
>
> *(d) In relation to* [redacted] *[Facebook, Inc.]* [redacted].
>
> *(e) In relation to* [redacted] *a number of changes have been made in relation to* [redacted].
>
> *(f) In relation to* [redacted] *[Facebook, Inc.] engineers* [redacted]*"*[108]

125. Post-incident reviews are among the measures taking into account the state of the art that FB-I and Facebook, Inc. would be expected to implement in order to ensure technical and organisational measures remain appropriate and to mitigate systemic weaknesses that may give rise to the recurrence of similar incidents. The DPC has not been provided with supporting documentary evidence associated with any of the post-incident reviews undertaken. This is notwithstanding that FB-I was asked, for example, in Query 8 in the Commencement Notice to provide, for each of the Breaches, "*detailed information and Relevant Supporting Documentary Evidence regarding any technical and organisational weaknesses FB-I has identified that may have contributed to all or any of the […] Breaches*." FB-I's response to Query 8, for each of the Breaches, was to the effect that FB-I was commencing a technical and organisational measures review (the Expert Review referred to at

[106] FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019), pages 1 and 2.
[107] FB-I's Response to the Draft Inquiry Report (22 May 2020), pages 45 to 46.
[108] FB-I's Response to the Draft Inquiry Report (22 May 2020), page 47. I have also had regard to the more detailed summary of these examples which was given in FB-I's Response to Queries 13 to 15 in the Commencement Notice (15 March 2019), pages 2 to 5.

paragraphs 31 to 35, above) and would endeavour to update the DPC in relation to outcomes from this review, as appropriate. It is not clear why FB-I did not consider it relevant to provide further details and supporting documentary evidence relating to the post-incident reviews undertaken following the twelve Breaches, providing insight into their content, how they were carried out, and how it was determined that the follow-up actions summarised in the quote at paragraph 124, above, would constitute appropriate security measures to prevent the recurrence of the issues that gave rise to the twelve Breaches the subject of this Inquiry, or similar issues.

126. I have had regard to FB-I's submissions on the above analysis, as it appeared in the Preliminary Draft Decision,[109] but I consider that no change to the previous paragraphs is warranted in light of the absence of any specific documentary materials detailing the actions taken, particularly on foot of the discovery of the Breaches in question.

Consideration of certain general issues raised in FB-I's Response to the Preliminary Draft Decision

127. In FB-I's submissions on the Preliminary Draft Decision, FB-I set out a number of arguments of a more general nature which it is necessary to summarise and address briefly below.

(1) FB-I has submitted that the accountability obligations under Articles 5(2) and 24(1) GDPR are non-prescriptive and permit controllers wide discretion in how they comply.[110] FB-I relied, *inter alia*, on the Article 29 Working Party's Opinion 3/2010 on the principle of accountability (13 July 2010), where it is stated that "*in determining the types of measures to be implemented, there is no option but "custom built" solutions. Indeed, the specific measures to be applied must be determined depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and the types of data. A one-size-fits-all approach would only force data controllers into structures that are unfitting and ultimately fail.*"[111] However, equally, I note the Article 29 Working Party's recognition that "*controllers must be able to tailor the measures to the concrete specifics of the data controller and the data processing operations in question.*" This is reflected in Article 24(1) GDPR, which requires that controllers implement appropriate technical and organisational measures to be able to demonstrate that processing is performed in accordance with the GDPR, *"[t]aking into account 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 person*". I have set out my assessment at paragraphs 56 to 71, above, relating to the significant risks associated with the processing for which FB-I's is a controller, in light of its nature, scope, context and purpose. I further note the Article 29 Working Party's acknowledgment that, *"in principle, large data controllers should implement stringent measures*" to ensure their accountability obligations are met. Even if the requirements of Articles 5(2) and 24(1) GDPR incorporate, by necessity, an element of scalability and flexibility, I do not agree that this can be relied on to avoid the consequences of a finding of infringement pin-pointing a failure to comply, in a specific case, with the obligations under Articles 5(2) and 24(1) GDPR.

(2) FB-I has also argued that, to the extent that the DPC has formed the view that FB-I did not comply with Articles 5(2) and 24(1) GDPR by having in place appropriate technical and organisational measures to be able to demonstrate that FB-I and Facebook, Inc.'s processing was in compliance with Articles 5(1)(f) and 32 in light of the twelve Breaches, the DPC's expectations are unrealistic

[109] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraphs 2.28 to 2.34, pages 22 to 24.
[110] See for example FB-I's Response to the Preliminary Draft Decision (21 July 2021), Executive Summary, paragraph 3, page 3 and Part C, paragraphs 1.4 to 1.7, pages 12 and 13.
[111] Article 29 Working Party's Opinion 3/2010 on the principle of accountability (13 July 2010), paragraph 45.

and unreasonable.[112] I wish to note, in this regard, that the DPC's expectation that a controller would be in a position to demonstrate (as required by Article 5(2) and Article 24(1) GDPR) that technical and organisational security measures for the purposes of Articles 5(1)(f) and 32 GDPR are implemented and adhered to in practice, by reference to contemporaneous records or documentation evidencing the actual activities carried out within the scope of such measures, is not unworkable in practice or unsupported by the GDPR. The DPC, as a supervisory authority, supervises other platforms of equivalent scale to FB-I and has identified compliance with the effective demonstration requirements (by means, for example, of contemporaneous documentation in relation to a specific incident) to the standard anticipated in other cases.

(3) FB-I has submitted, in addition, that, at the relevant time (i.e. in the period between 7 June 2018 and 4 December 2018 when the twelve Breaches were notified to the DPC), the accountability obligations under Articles 5(2) and 24(1) GDPR were unclear and insufficient guidance had been made available by the Article 29 Working Party, the EDPB or the DPC to enable FB-I to understand its obligations as a controller in this regard.[113] However, it would not be appropriate for the DPC to refrain from monitoring and enforcing the application of particular Articles of the GDPR until such time as they become the subject of detailed published guidance by the EDPB, or interpretation by the Irish or EU courts. While it is among the tasks of the DPC as a supervisory authority to promote the awareness of controllers and processors of their obligations under the GDPR, in accordance with Article 57(1)(d) GDPR (which the DPC carries out by, *inter alia*, publishing guidance for controllers and processors on its website), it has consistently been the DPC's position that it is the responsibility of each individual controller to understand the nature and extent of its obligations under the GDPR (where appropriate, with the assistance of legal advice) and to demonstrate that its processing is performed in compliance with the GDPR and the 2018 Act, having regard to the particular context, circumstances and characteristics of that controller's processing.

[112] See for example FB-I's Response to the Preliminary Draft Decision (21 July 2021), Executive Summary, paragraph 3, page 3 and Part C, paragraph 2.2, page 14, paragraph 2.5, page 16, paragraph 2.12, page 18, and paragraph 2.21, page 20.

[113] See for example FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part C, paragraphs 1.8 and 1.9, page 13, and paragraph 2.1, page 14.

Finding of Infringement

128. In light of the analysis outlined above, I make the following finding of infringement:

> FINDING OF INFRINGEMENT
>
> Contrary to Articles 5(2) and 24(1) GDPR, FB-I did not implement appropriate technical and organisational measures in the period between 7 June 2018 and 4 December 2018 in order to be able to demonstrate that the processing of EU users' personal data by FB-I and Facebook, Inc. relevant to the twelve Breaches was performed in accordance with the GDPR (specifically in accordance with Articles 5(1)(f) and 32(1) GDPR), insofar as FB-I was required to demonstrate, in the context of this Inquiry, that it had in place and that it implemented:
>
> (I) an appropriate risk assessment framework,
>
> (II) effective software vulnerability and bug management measures, and
>
> (III) effective incident response policies and procedures,
>
> as part of appropriate technical and organisational security measures under Articles 5(1)(f) and 32(1) GDPR to ensure a level of security that, in practice, was appropriate to the risks of FB-I and Facebook, Inc.'s processing (to include the risk of software bugs occurring in the codebase underlying Facebook, Inc.'s systems resulting in personal data breaches within the meaning of Article 4(12) GDPR).

129. In making the above finding, my conclusion differs from the views of the inquiry team, as expressed in the Final Inquiry Report in two main respects:

130. First, I have declined to make a finding that FB-I infringed outright its obligations under Articles 5(1)(f) and 32 GDPR. I do not consider that the information obtained in the course of this Inquiry establishes that FB-I and Facebook, Inc. failed, in the period between 7 June 2018 and 4 December 2018, to have in place appropriate technical and organisational security measures capable of underpinning a level of security appropriate to the risk associated with the processing, as required by Articles 5(1)(f) and 32 GDPR. As I have observed in the course of this Decision, I consider that the information and supporting documentary evidence provided by FB-I in the Inquiry is indicative of an approach to security at FB-I and Facebook, Inc. 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. Rather, the fundamental concern arising in this Inquiry is FB-I's failure to have in place appropriate technical and organisational measures such as would enable it to readily demonstrate the security measures that it implemented in practice to protect EU users' data in the context of the twelve Breaches the subject of this Inquiry. For the avoidance of doubt, this conclusion does not amount to a finding of compliance with Article 5(1)(f) or 32 GDPR in respect of any or all of the technical and organisational security measures referred to herein. Further, it is strictly without prejudice to any analysis or findings relating to FB-I's compliance with Articles 5(1)(f) and 32 GDPR in the time period at issue in this Inquiry, which may subsequently be made by the DPC in the context of other inquiries or regulatory activities which are currently ongoing at the date of this Decision.

131. Second, I have deemed it appropriate to make one overarching finding of infringement of Articles 5(2) and 24(1) GDPR arising from the issues raised by this Inquiry, by contrast with the approach taken in the Final Inquiry Report of finding multiple separate infringements by reference to each of the twelve Breaches. In doing so, I have taken particular account of the need to exercise my powers under the GDPR and the 2018 Act in a manner which is proportionate in all the circumstances.

DECISION ON CORRECTIVE POWERS IN ACCORDANCE WITH SECTION 111(2) OF THE 2018 ACT

132. I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, the reasons for my finding that, in respect of the in the period between 7 June 2018 and 4 December 2018, FB-I is responsible for an infringement of Articles 5(2) and 24(1) GDPR.

133. Under Section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with Section 111(1)(a) of the 2018 Act), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned, and, if so, the corrective power to be exercised. Having carefully considered the infringement identified in this Decision, together with FB-I's submissions on my proposed exercise of corrective powers in the Preliminary Draft Decision – which, it is necessary to state, have been made without prejudice to FB-I's position in relation to the infringement – I have decided to exercise corrective powers in accordance with Section 115 of the 2018 Act and Article 58(2) GDPR.

Corrective power to be exercised

134. I have decided to impose an administrative fine pursuant to Article 58(2)(i) and Article 83 GDPR in respect of FB-I's infringement of Article 5(2) GDPR, as identified in this Decision. I set out below the reasons for my decision, in this regard, having considered all of the corrective powers set out in Article 58(2) GDPR.

135. A matter which it is necessary to address in light of the infringement identified here is that Article 83(1) GDPR refers to the power of supervisory authorities to impose administrative fines "*in respect of infringements of [the GDPR] referred to in paragraphs 4, 5 and 6*". Although I have included in my finding of infringement a finding in relation to FB-I's infringement of Article 24(1) GDPR, that provision is not referred to in Articles 83(4), (5) or (6) GDPR. Accordingly, albeit that the analysis of the infringements of Articles 24(1) and 5(2) GDPR are necessarily interlinked in this Decision due to the close relationship and common material scope of those two provisions, the administrative fine ultimately imposed here is addressed to the infringement of Article 5(2) GDPR only.

136. In this connection, FB-I has submitted that:

> *"[…], the GDPR does not allow for an administrative fine to be based on an infringement of Article 24 GDPR. This is reflective of the fact that an infringement of Article 24(1) cannot give rise to risk or damage to data subjects and as such cannot warrant the imposition of a fine. Given that the Article 5(2) infringement alleged in this Inquiry is connected entirely with an Article 24(1) infringement, it is unclear on what basis the DPC seeks to impose such a fine."*[114]

137. I wish to record that I do not agree with the above submission in circumstances where there is no indication in Article 83 GDPR or otherwise that the legislature intended to exclude an infringement of Article 5(2) GDPR from those infringements of the GDPR which ought to be sanctioned by way of

[114] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.10, page 36.

an administrative fine. I note, in particular, that infringements of Article 5 GDPR generally are expressly included in the list of infringements in Article 85(5)(a) which may attract administrative fines of up to €20 million or, in the case of undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Decision not to exercise power to make the order previously proposed under Article 58(2)(d) GDPR

138. A further matter which it is necessary record is that, in the Preliminary Draft Decision, I initially proposed – on a provisional basis – to exercise the power of the DPC to make an order under Article 58(2)(d) GDPR directed towards requiring FB-I to take measures to bring the processing the subject of this Inquiry into compliance with Article 5(2) and 24(1) GDPR.

139. In that regard, I had taken into account the information and submissions FB-I provided to the DPC relating to the improvements it has made to its technical and organisational measures as a result of the Expert Review which I have referred to above. As set out at paragraphs 31 to 35, above, FB-I informed the inquiry team, following the commencement of the Inquiry, that, as of 4 February 2019, FB-I (via its external lawyers) had instructed an expert technologist on a privileged basis to conduct an Expert Review of FB-I's technical and organisational security measures. Correspondence was exchanged between FB-I and the inquiry team relating to the Expert Review during the course of the Inquiry. As indicated previously at paragraph 35, FB-I provided an update to the DPC following the completion of the Expert Review by way of letter dated 23 March 2020 detailing, in overview (and without prejudice to its privileged nature), the scope of the review and the measures FB-I proposed to implement on foot of it, as well as informing the DPC that a review of Facebook, Inc.'s coding practices had been carried out. Further information in relation to the Expert Review was provided in FB-I's Response to the Draft Inquiry Report (22 May 2020) (in particular pages 47 to 51 and Annex 3 and Annex 4 thereof). Annex 3 consisted of a document entitled [redacted]' dated [redacted] The documentation comprising Annex 4 was provided to the DPC separately on 9 June 2020. The relevant documentation supplied as part of Annex 3 and Annex 4 is as follows:

Document	Date
[redacted]	

140. In view of the information and submissions provided by FB-I in connection with the Expert Review, I had, in the Preliminary Draft Decision, proposed an order under Article 58(2)(d) GDPR, requiring FB-I to examine, reassess and update the enhanced measures adopted on foot of the Expert Review, which are outlined in Annex 4 to its Response to the Draft Inquiry Report (22 May 2020), in light of

the provisional finding of infringement of Articles 5(2) and Article 24(1) identified in the Preliminary Draft Decision.

141. With its submissions on the Preliminary Draft Decision, FB-I provided, at Annexes A and B, revised and updated versions of several of the documents provided to the DPC on 9 June 2020, as follows:

Document	Date
[redacted]	[redacted]

142. Having reviewed the updated documentation provided as Annexes to FB-I's submissions on the Preliminary Draft Decision, relating to the enhanced technical and organisational measures FB-I has implemented in the course of the Inquiry, I have decided not to proceed to exercise my power to impose on FB-I the order pursuant to Article 58(2)(d) GDPR that I had proposed in the Preliminary Draft Decision. I am satisfied, at present, that the documentation most recently submitted by FB-I provides sufficient assurance of the efforts taken by FB-I to address the concerns identified in this Decision in the period subsequent to the commencement of this Inquiry that the order I had proposed to make under Article 58(2)(d) GDPR is not currently necessary. This determination is strictly without prejudice to any analysis or findings relating to FB-I's ability to demonstrate the actual implementation of the enhanced measures in practice which may subsequently be made by the DPC in the context of other inquiries or regulatory activities which are currently ongoing at the date of this Decision. While FB-I's submissions relating to the proposed order under Article 58(2)(d) GDPR[115] addressed a number of arguments as to why FB-I did not consider that the proposed order was appropriate, necessary or proportionate in this particular case, in view of my decision to not to proceed with the proposed order in this instance, I consider it unnecessary to go on to separately consider each of those arguments here.

Decision relating to Administrative Fine under Articles 58(2)(i) and 83 GDPR

143. As set out above, I have decided to exercise my power to impose an administrative fine under Article 58(2)(i) and 83 GDPR.

144. Article 83(2) GDPR provides that, for the purpose of deciding *whether* to impose an administrative fine and deciding on the *amount* of the administrative fine to be applied in FB-I's individual case, I am required to have due regard to the following matters:

[115] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraphs 1.1 to 2.12, pages 31 to 34.

(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.

145. Article 83(1) provides that I am required to ensure that the imposition of administrative fines pursuant to Article 83, in respect of infringements of the GDPR referred to in Articles 83(4), (5) and (6), is, in each individual case, "*effective, proportionate and dissuasive*".

146. Further, 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." As I have considered the imposition of an administrative fine in respect of one finding of infringement of Article 5(2) GDPR only, the application of Article 83(3) does not fall to be considered here.

147. In the following section, I outline my views in relation to each of the matters referred to in Article 83(2) GDPR as they apply to the infringement of Article 5(2) GDPR which I have identified above.

Article 83(2)(a) – the nature, gravity and duration of the infringement(s) 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

148. The *nature of the infringement* has been described at paragraphs 80 to 126, above, leading to the finding that FB-I, in the period between 7 June 2018 and 4 December 2018, was responsible for an infringement of Article 5(2) GDPR (as well as Article 24(1) GDPR, which, however, as clarified above, does not fall for consideration, as regards the imposition of an administrative fine under Articles 58(2)(i) and 83 GDPR). The nature of the infringement relates to FB-I's accountability obligations as a controller under the GDPR, in terms of FB-I's ability, in the relevant period, to be able to demonstrate that the processing of EU users' personal data by FB-I and Facebook, Inc., relevant to the twelve Breaches, was performed in accordance with the GDPR (specifically in accordance with Articles 5(1)(f) and 32(1) GDPR). It is important to acknowledge, in this regard, that the infringement does not relate to the substance or underlying causes of any of the twelve Breaches which prompted the initiation of this Inquiry, and does not include any finding that FB-I failed to comply with Articles 5(1)(f) or 32 GDPR. This has been an important consideration in my assessment of the overall level of the administrative fine.

149. The *duration of the infringement* corresponds to the time period under examination in the Inquiry, namely the period of approximately 6 months between 7 June 2018 and 4 December 2018. FB-I has outlined its view that the infringement was of limited duration and its duration cannot be a factor that either warrants the imposition of an administrative fine or increases the amount of any such fine. FB-I has also submitted that the duration of infringement should, in fact, be considered a mitigating factor in light of the fact that FB-I already started enhancing its technical and organisational measures in January 2019, and the proactive steps taken by FB-I to limit the duration of any alleged infringement must be taken into account by the DPC as a mitigating factor.[116] In the circumstances, I consider the duration of the infringement to be neither aggravating nor mitigating in terms of the level of the administrative fine. I have separately taken into account the changes to FB-I's technical measures on foot of the Expert Review, from January 2019 onwards, as a mitigating factor under Article 83(2)(c) below.

150. The *nature, scope and purpose of the processing* to take into consideration, in this context, is not just the processing operations specifically giving rise to the Breaches, or the causes thereof, but rather the scope of the underlying processing involved in providing the Facebook and Instagram services to EU users. I have outlined, at paragraph 60 above, the matters I consider relevant when taking into account the nature, scope and purpose of the processing carried out in the context of the Facebook and Instagram services and I consider that analysis to also be relevant here. In summary, the matters I have taken into account, in this regard, include that Facebook and Instagram are popular and widely used social media services, the large scale of the processing, as indicated by the number of EU users of Facebook and Instagram services in Q4 2018, and the description of Facebook, Inc.'s codebase in terms of its size and complexity and that the processing carried out for the purpose of providing the Facebook and Instagram services involves large numbers of data subjects, as well as a wide range of types and categories of personal data (potentially including children's data and special category data in some circumstances) in high volumes. The scale of the processing for which FB-I is responsible as a controller within the meaning of Article 4(7) GDPR is a significant factor to which I have attributed due weight in the overall assessment of the administrative fine.

151. The *number of data subjects affected and the level of damage suffered by them* is a further matter which may be taken into account under Article 83(2)(a). It is clear that this aspect of the Article 83(2)(a) criterion refers to any damage which may have been suffered by data subjects as a result of the *infringement* of the GDPR[117] identified in this Decision, that is, the infringement of Article 5(2)

[116] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.16 to 3.17, page 37.

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

GDPR. In this regard, FB-I has submitted that the infringement of Article 5(2) GDPR identified in this Decision (which concerns a failure to have in place appropriate technical and organisational measures to enable FB-I to readily demonstrate to the DPC the security measures that it implemented in practice in the context of the Breaches) did not, itself, directly affect or cause damage to EU users.[118] Rather, it is a failure relating to FB-I's obligations of responsibility and accountability as a controller under the GDPR. Having reviewed FB-I's submissions in respect of this issue, I am minded to agree with this view. Consequently, I accept that it is not relevant to draw into account, in this context, the number of EU users affected by the twelve Breaches which prompted this Inquiry (which, as set out at paragraph 24 above, has been estimated by FB-I at approximately [redacted]) or, further, my analysis at paragraphs 63 to 71, above, relating to the damage to EU users which likely occurred as a result of the twelve Breaches, given such damage does not flow or result directly from the infringement of Article 5(2) GDPR which is the subject of the finding set out above at paragraph 128.[119] Accordingly, these matters cannot be taken into account as aggravating factors which would tend to increase the level of the administrative fine. Contrary to FB-I's submission, however, I do not agree that, to the extent that the infringement of Article 5(2) GDPR did not directly affect or cause damage to data subjects, this should be treated as a mitigating factor. This arises because of the nature of the breach of the obligation under Article 5(2) GDPR itself, rather than any other circumstance or conduct on the part of FB-I which could be viewed as mitigating.

152. As to the *gravity of the infringement* identified in this Decision, I have taken into account each of the matters outlined in the previous paragraphs relating to the nature, scope and purpose of Facebook, Inc.'s and FB-I's processing, and the nature and duration of the infringement. In assessing the gravity of the infringement, I have had regard, in particular, to the risks to the rights and freedoms for EU users associated with the scale of FB-I's processing. I have additionally had regard to the fact that the infringement of Article 5(2) GDPR identified in this Decision gives rise to a real and significant concern in relation to FB-I's ability to provide the DPC with sufficient information to enable the DPC to effectively exercise its supervisory powers in respect of FB-I's and Facebook, Inc.'s processing of the personal data of EU users, which concern is heightened in light of the risks to EU users that the processing underlying Facebook and Instagram services entails. In light of these matters, I have concluded that the infringement of Article 5(2) GDPR identified in this Decision is a moderately severe infringement that may be estimated to be approximately at the midpoint on the scale of potential gravity for an infringement of this nature, in view of all the circumstances. I note that FB-I considers that the infringement of Article 5(2) GDPR should be considered at the low end of the scale of gravity of an accountability infringement, but I do not consider that FB-I's submissions on this point provide a basis for altering my assessment of this criterion.[120]

Article 83(2)(b) – the intentional or negligent character of the infringement

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

> *"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no*

---

that "*If damages have been or are likely to be suffered due to the infringement of the Regulation then the supervisory authority should take this into account in its choice of corrective measure, although the supervisory authority itself is not competent to award the specific compensation for the damage suffered.*"

[118] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.18, page 37.

[119] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.19, page 38.

[120] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraphs 3.13 to 3.15, page 37.

intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."[121]

154. That guidance further provides that:

> *"[…] circumstances, 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.*
>
> *Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources. Routines and documentation of processing activities follow a risk-based approach according to the Regulation."*[122]

155. In the present circumstances, I do not consider that the infringement was of an intentional or wilful nature. However, I do consider that there was a negligent character to the infringement. In light of the nature, scope and purposes of the processing involved in providing the Facebook and Instagram services to EU users for which FB-I is a controller, the infringement identified in this Decision leads me to consider that FB-I's conduct fell below the standard of responsibility and accountability that a supervisory authority would expect of a controller in FB-I's position, taking into account the risk-based approach envisaged by the GDPR. Processing of personal data is central to FB-I and Facebook, Inc.'s business and it is legitimate for the DPC to expect that FB-I should have advanced and effective accountability measures in place to enable FB-I to demonstrate compliance with the requirements of the GDPR. In other words, my view is that FB-I *ought to have known* of its obligations, as regards the requirement for it to implement sufficient measures that would enable it to demonstrate compliance with its obligations under the GDPR. This is particularly the case given FB-I's size and the resources available to it. I note that FB-I disagreed with this view, stating *"[t]he requirements on what documentation was needed during the Relevant Period to readily demonstrate GDPR compliance were unclear and [FB-I] had already taken substantial steps to comply to the best of its knowledge with what Article 5(2) required"*[123] However, I am not persuaded that FB-I's submissions warrant a change in my approach to this criterion. I have treated the negligent character of the infringement as an aggravating factor. I further note FB-I's submission[124] that negligence should be "a neutral factor, at most", in circumstances where the Portuguese supervisory authority, further to the circulation of the Article 60 Draft for the purpose of Article 60(4) GDPR, expressed the view that an infringement must be classified as either negligent or intentional and cannot, otherwise, be classified as neither negligent nor intentional. I disagree with FB-I's view, in this regard. As already noted, above, my view is that FB-I ought to have known of its obligations, particularly in light of its size and the resources available to it. That being the case, it is reasonable for me to assess the extent of FB-I's shortcomings, in terms of what it failed to do, so as to determine the degree to which FB-I might be said to have been negligent. In the circumstances of this particular inquiry, I remain of the view that it is not only appropriate for me to treat the negligent character of the infringement as an aggravating factor for the purpose of this Article 83(2)(b) assessment, but to attribute medium weight to it when doing so.

---

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

[122] Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (3 October 2017) (endorsed by the EDPB on 25 May 2018), page 12.

[123] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.20, page 38.

[124] FB-I's submissions dated 1 February 2022, entitled "Response to the [DPC's] amended draft decision received on 21 January 2022", paragraphs 3.21 and 3.22, page 13

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

156. In the Preliminary Draft Decision, I took account of the information FB-I provided in the Inquiry in relation to the remediation and mitigation measures taken by FB-I and Facebook, Inc. in respect of each of the twelve Breaches (notwithstanding my concerns as to the deficiencies in FB-I's ability to demonstrate such measures as required by Article 5(2) GDPR) as mitigating factors. However, I now accept, in light of FB-I's submissions concerning Article 83(2)(a) above, that the effect on, and damage caused to, EU users arising from the twelve Breaches which gave rise to the Inquiry is not a relevant matter to consider in the context of the assessment of the infringement of Article 5(2) GDPR. It follows, similarly, that the measures taken by FB-I and Facebook, Inc. at the time the twelve Breaches occurred, to mitigate or remediate any effect on, or damage to, EU users, should not be considered relevant under the Article 83(2)(c) criterion in connection with the infringement of Article 5(2) GDPR. Accordingly, these matters have not been taken into account as mitigating factors which would tend to reduce the level of the administrative fine.

157. A matter which it is appropriate to address under Article 83(2)(c) GDPR is the Expert Review and the information provided by FB-I concerning changes or improvements FB-I made to its technical and organisational security measures following the commencement of the Inquiry. I consider the fact that FB-I arranged for the Expert Review to be undertaken following the commencement of the Inquiry is demonstrative of positive efforts on the part of FB-I to reassess and make changes to the technical and organisational measures applicable to the Facebook and Instagram services to better meet the requirements of Article 5(2) GDPR. I have taken this into account and afforded it due weight, as a mitigating factor under Article 83(2)(c) GDPR. Contrary to FB-I's submissions,[125] however, I do not consider that I am obliged to specifically quantify the value of this, or any other, mitigating factor as a percentage or proportion of the overall monetary value of the administrative fine. Whereas the DPC has, on occasion, taken a more granular approach to the quantification of mitigating factors in certain of its previous (domestic) inquiries for which decisions have been published, the DPC does not agree that the absence of a similar level of granularity, in any other inquiry, constitutes a material difference or inconsistency in approach that is in any sense unfair to FB-I.

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

158. The Article 29 Working Party has interpreted Article 83(2)(d) to as requiring the supervisory authority to answer the question of "*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 [GDPR]*".[126] As appears from the analysis of set out above, I consider that the failure to have in place systems and procedures, in accordance with Article 5(2) GDPR, for maintaining appropriate documentation and records to enable FB-I and Facebook, Inc. to demonstrate the effectiveness of their technical and organisational measures had the effect of limiting the DPC's ability to fully supervise and verify the extent of FB-I's compliance with its obligations under the GDPR for the period 7 June 2018 to 4 December 2018. I consider that this fell short of the level of responsibility for compliance with the GDPR which might be expected of a controller involved in processing at the

[125] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.25, page 39.
[126] Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (3 October 2017) (endorsed by the EDPB on 25 May 2018), page 13.

scale and complexity of that associated with the Facebook and Instagram services, which is aggravating in this context. I note FB-I's observations on this criterion, whereby FB-I disagrees with the DPC's view that FB-I did not have systems and procedures in place to demonstrate the effectiveness of its technical and organisational measures during the relevant period, and argues that the Article 83(2)(d) factor should be treated as neutral. [127] However, I have not considered it necessary to alter my views in this respect.

Article 83(2)(e) – any relevant previous infringements by the controller or processor

159. No relevant previous infringements by FB-I arise for consideration in this context and, accordingly, I propose to view this as neither an aggravating nor a mitigating factor. FB-I has taken issue with this in its submissions, on the basis that this approach is inconsistent with certain published decisions of the DPC in previous (domestic) inquiries.[128] However, it is necessary to appreciate that the DPC's approach to the presence or absence of relevant previous infringements (for the purpose of the Article 83(2)(e) assessment) differs, depending, inter alia, on the contexts of different types of controllers, particularly as concerns the scale of the processing at issue. Unlike the position with the inquiries referred to in FB-I's submissions, cross-border inquiries into larger social media platforms such as Facebook and Instagram generally concern controllers or processors with significant multinational operations and extensive resources available to them, including large in-house compliance teams. Such controllers are further likely to be engaged in business activities that are uniquely dependent on the large scale processing of personal data. The DPC's view is that the size and scale of such controllers, the level of dependency on data processing and the extensive resources that are available to them necessitate a different approach to the absence of previous relevant infringements.

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

160. I acknowledge FB-I's cooperation with the DPC during the course of the Inquiry. However, I note that FB-I was, in any event, under a duty, in light of Article 31 GDPR, to cooperate, on request, with the supervisory authority in the performance of its tasks. I wish to note that while (as FB-I has submitted) the initiation of an Expert Review following the commencement of the Inquiry may be viewed as a step towards remedying the infringement of Article 5(2) GDPR described in this Decision and to mitigating its possible adverse effects,[129] the initiation of the Expert Review has separately been taken into account as a mitigating factor under Article 83(2)(c) above.

Article 83(2)(g) – the categories of personal data affected by the infringement

161. As set out previously, I consider that the processing involved in providing the Facebook and Instagram services involves a wide range of types and categories of personal data (potentially including children's data and special category data in some circumstances), in high volumes. In line with my approach under Article 83(2)(a), however, I accept that the infringement of Article 5(2) identified in this Decision may not be said to "*affect*" the personal data of the EU users concerned by the twelve Breaches the subject of the Inquiry. Notwithstanding FB-I's view[130], however, I do not consider that this should be characterised as a mitigating factor. Rather, the nature of an infringement of Article

[127] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.27 to 3.28, page 39.
[128] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.29, page 39.
[129]FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.32, page 40.
[130] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.33, page 40.

5(2) GDPR, in the circumstances of this particular Inquiry, means that the categories of personal data affected by the infringement should be treated as neither aggravating nor mitigating in this case.

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

162. The infringement of Article 5(2) GDPR identified in this Decision became known to the DPC in the course of an Inquiry that commenced on 11 December 2018 in respect of the twelve Breaches which were notified to the DPC by or on behalf FB-I on dates between 7 June 2018 and 4 December 2018. However, the notification of the twelve Breaches under Article 33(1) GDPR does not equate to notification of the "*infringement*" at issue for the purpose of the Article 83(2) criteria. Rather, the twelve Breaches prompted the DPC to begin an inquiry process, seeking to establish FB-I's compliance with different elements of its obligations under the GDPR in the context of the processing involved in providing the Facebook and Instagram services to EU users. I have considered FB-I's submissions on this issue[131] but I view this criterion as relevant only to the extent that it is necessary to acknowledge the context and background to the Inquiry, and have regarded it as neither aggravating nor mitigating.

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

163. FB-I submits that it has never been subject to a finding of infringement of the GDPR and has never been subject to corrective measures under Article 58(2) GDPR and that this must be a mitigating factor in the DPC's assessment. [132] I note FB-I's submission on this issue but I consider the fact that no previous measures under Article 58(2) GDPR arise for consideration to be neither aggravating nor mitigating.

Article 83(2)(j) – adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

164. FB-I submits that it has not adhered to relevant codes of conduct or certifications because none exist, but that that its approach to accountability aligns with the approach adopted by industry peers.[133] I consider that the criterion at Article 83(2)(j) is simply not applicable in this case, and it is unnecessary to address the issue further.

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

165. I am not aware of financial benefits gained or losses avoided by FB-I, whether directly or indirectly, from the infringement identified in this Decision. I note FB-I's view that this matter counts as a mitigating factor, [134] however, I do not agree with this approach.

[131] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.35 to 3.36, page 41.
[132] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.37, page 41.
[133] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.38, page 41.
[134] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.39, page 41.

166. I am satisfied that the matters set out under Articles 83(2)(a) to (k), above, give a full account of the factors to which I should have due regard in the context of Article 83(2) GDPR.

Decision as to whether to impose an administrative fine

167. Having taken into account each of the criteria in Article 83(2) GDPR, I have decided, as indicated above, that it is appropriate to impose on FB-I an administrative fine in respect of the finding of infringement of Article 5(2) GDPR made in this Decision. I have additionally taken into account the requirement, in Article 83(1) GDPR, for any administrative fine imposed to be "*effective, proportionate and dissuasive*" in each individual case. In this regard, the Article 29 Working Party has observed that:

> *"Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to re-establish compliance with the rules, or to punish unlawful behaviour (or both)."*[135]

168. In this case, I consider that the imposition of an administrative fine is necessary in order to effectively meet the objective of ensuring that FB-I continues its efforts towards achieving compliance with Article 5(2) GDPR in light of the analysis in this Decision, and the objective of dissuading FB-I from allowing further, similar infringements to that identified in this Decision to recur in the future.

Decision as to the amount of the administrative fine to be imposed

169. In circumstances where I have decided that the infringement of Article 5(2) GDPR which has been identified in this Decision warrants the imposition of an administrative fine, I must, therefore, next proceed to decide on the amount of the administrative fine, in light of both my consideration of the factors set out above under Articles 83(2)(a) to (k) GDPR, and also in light of the obligation under Article 83(1) to ensure that the administrative fine imposed in this case is "*effective, proportionate and dissuasive*".

Parameters for the administrative fine

170. In deciding on the amount of the fine which is to be imposed in respect of the infringement of Article 5(2) GDPR, it is relevant to have regard to Articles 83(4) and (5) GDPR, which provide for a maximum permitted level or 'cap' in respect of administrative fines imposed for specified provisions of the GDPR. In this instance, it is relevant that Article 83(5) GDPR provides that infringements of Article 5 GDPR (including Article 5(2) GDPR) shall, in accordance with Article 83(2), be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Definition of "undertaking" in the context of Article 83(5) GDPR

[135] Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (3 October 2017) (endorsed by the EDPB on 25 May 2018), page 6.

171. Article 83(5) GDPR requires me to consider, for the purpose of determining the appropriate level of the administrative fine, the definition of an "*undertaking*".

172. Recital 150 GDPR states as follows:

> *"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. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine."*

173. The CJEU, in EU competition law, has consistently held that the definition of an "undertaking" covers "any entity engaged in an economic activity, regardless of the legal status of that entity and the way in which it is financed".[136] Further, the concept of an undertaking is to be "understood as covering an economic unit, even if, from a legal perspective, that unit is made up of a number of natural or legal persons"[137].

174. The case law of the CJEU indicates that the conduct of a subsidiary may be imputed to the parent company, in particular, where, although having a separate legal personality, that subsidiary does not decide independently upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by the parent company, having regard, in particular, to the economic, organisational and legal links between them. That follows because, in such a situation, the parent company and its subsidiary form a single economic unit and therefore form a single undertaking.[138] Where a subsidiary is wholly owned (or almost wholly owned)[139] by a parent company, there is a rebuttable presumption that the parent company in fact exercises a decisive influence over the conduct of its subsidiary[140] so that, together, they constitute a single undertaking.

175. The CJEU has further clarified that, in the specific case where a holding company wholly owns all of the capital of an interposed company which, in turn, holds the entire capital of a subsidiary of its group which has committed an infringement of EU competition law, there is a rebuttable presumption that that holding company exercises decisive influence over the conduct of the interposed company and also, indirectly, via that interposed company, over the conduct of that subsidiary.[141]

176. I have had regard to FB-I's Director's Report and Financial Statements for the Financial Year ended 31 December 2019, which are available from the Companies Registration Office and are dated December 2020. This is the most recently filed Director's Report and Financial Statements as at the date of this decision. On page 3 of the document, it is stated that:

---

[136] Judgments of the CJEU of 23 April 1991, *Höfner and Elser*, C-41/90, EU:C:1991:161, paragraph 21.

[137] Judgment of the CJEU of 10 April 2014, *Areva v. Commission,* C-247/11 etc., EU:C:2014:257, paragraph 125, and judgment of 27 April 2017, *Akzo Nobel v. Commission,* C-516/15, EU:C:2017:314, paragraphs 47 and 48.

[138] Judgment of the CJEU of 10 September 2009, *Akzo Nobel v. Commission*, C-97/08, EU:C:2009:536, paragraphs 58 and 59.

[139] Judgment of the CJEU of 8 May 2013, *Eni v. Commission*, C-508/11, EU:C:2013:289, paragraph 47, and judgment of 27 April 2017, *Akzo Nobel v. Commission*, C-516/15, EU:C:2017:314, paragraph 54.

[140] Judgment of the CJEU of 10 September 2009, *Akzo Nobel v. Commission*, C-97/08, EU:C:2009:536, paragraphs 60 to 61.

[141] Judgment of the CJEU of 20 January 2011, *General Química v. Commission* , C-90/09, EU:C:2011:21, paragraph 88 and judgment of the CJEU of 8 May 2013, *Eni v. Commission*, C-508/11, EU:C:2013:289, paragraph 48.

> *"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."*

177. At Note 24 to the Financial Statements, on page 39, it is stated that:

> *"At 31 December 2019, the company is a wholly-owned subsidiary of Facebook International Operations Limited, a company incorporated in the Republic of Ireland, its registered office being 4 Grand Canal Square, Grand Canal Harbour, Dublin 2.*
>
> *The ultimate holding company and ultimate controlling party is Facebook, Inc., a company incorporated in Wilmington, Delaware, United States of America. 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."*

178. I understand that the above has remained the position in the interim. I note, in this connection, that the same position was stated in Facebook Ireland Limited's Directors' Report and Financial Statements for the year ended 31 December 2018, which is dated November 2019.

179. It appears, in light of the above, that a rebuttable presumption arises to the effect that Facebook, Inc. does in fact exercise a decisive influence over FB-I's conduct. It follows that Facebook, Inc. and FB-I are to be viewed together as one undertaking for the purpose of calculating the administrative fine under Article 83 GDPR. Accordingly, under Article 83(5) GDPR, the administrative fine imposed in this Decision should be subject to an upper limit or 'cap' of 4% of the total worldwide annual turnover of the preceding financial year of the relevant undertaking, which includes Facebook, Inc. and FB-I.

180. In its submissions on the Preliminary Draft Decision, FB-I disagrees with the position set out above and argues that the relevant "*undertaking*" for the purposes of Articles 83(4) to (6) GDPR is FB-I alone, as follows:[142]

> *[…] the DPC's views on the question of the relevant "undertaking" for the purposes of Articles 83(4) to (6) GDPR as set out in the PDD are wrong as a matter of fact and law. In particular:*
>
> *(a) [FB-I] disagrees with the DPC's approach to the assessment of whether an entity is in a position to exercise "decisive influence" over [FB-I]'s "behaviour on the market" in the context of the GDPR. How such competition law principles are applied in the very different statutory context of the GDPR is very much an open question.*
>
> *(b) [FB-I] does in fact operate with sufficient independence on the market that it should not be conflated with [Facebook, Inc.] on the basis of an assessment of "behaviour on the market" in the context of the GDPR. In other words, any presumption of decisive influence can be rebutted on the facts.*
>
> *(c) In particular:*

[142] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.39, page 41 to 42.

(i) The competition law concept of decisive influence does not directly translate in the context of the GDPR, which pursues different objectives to Articles 101 / 102 of the Treaty on the Functioning of the European Union. For example, a subsidiary's "conduct on the market" is of particular significance in the competition law context because it is the subsidiary's (anti-competitive) conduct on the market that distorts competition (and it is then the value of sales of goods or services to which that alleged anticompetitive conduct relates that is used to establish the 'basic amount' of a fine). "Conduct on the market" does not have the same significance in a data protection context, where it is the controller's or processor's data processing activities that have the potential to impact on data subjects' privacy rights.

(ii) For the competition law concept of decisive influence to have any real meaning in the context of the GDPR it must therefore be adapted accordingly, in a similar way to how the concept of "dominant influence" in Recital 37 GDPR has been adapted (e.g., from its European Works Council form) by encompassing, for example, the ability to control the processing activities of subsidiaries.

(iii) Accordingly, in order to determine whether [Facebook, Inc.] exercises decisive influence over [FB-I]'s "conduct on the market" for the purposes of the GDPR, the DPC's analysis should properly focus on [FB-I]'s data processing activities and the related decision making about personal data processed by [FB-I]. [FB-I] submits that this is the relevant behaviour to be considered when assessing "decisive influence" on behaviour in relation to Articles 83(4) to (6) GDPR.

(iv) As the DPC is aware, and as noted in the PDD,117 [FB-I] is the controller for user data processed for the purposes of providing the Services in the EU.

(d) Accordingly, [Facebook, Inc.] cannot properly be said to have "decisive influence" when that term is considered in a GDPR context.

181. I do not accept the alternative interpretation suggested by FB-I, for the following reasons:

(1) Recital 150 GDPR expressly states that "[w]here 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." Recital 150 indicates an intention by the EU legislature to incorporate the definition of "undertaking" from EU competition law into the GDPR insofar as the term "undertaking" is used in connection with the imposition of administrative fines. This arises, in particular, in Articles 83(4) to (6) GDPR.

(2) The concept of an "*undertaking*" in Articles 101 and 102 TFEU is not defined in the text of those articles, but, rather, has developed by interpretion in the case law of the EU courts in the field of EU competition law. The concept of "*decisive influence*" has been developed by the CJEU in that context for the purpose of determining whether one or more natural or legal persons constitute a single economic entity. It is not apparent, from the text of the GDPR, whether or how the concept of "*decisive influence*" is to be adapted or applied differently in the statutory context of the GDPR. In particular, it is not clearly indicated that the exercise of determining whether one entity exerts "*decisive influence*" over a another's conduct on the market is to be conflated with the question of which of the two entities takes decisions concerning data processing activities for the purposes of the GDPR. If it had been the intention of the EU legislature to align the definition of the relevant "*undertaking*" for the purposes of Article 83(4) to (6) GDPR with the definition of a "*controller*" within the meaning of Article 4(7) GDPR – that is, the *"natural or legal person […] which, alone or jointly with others, determines the purposes and means of the*

processing of personal data", it would presumably have done so explicitly. As it stands, there is no clear basis in the text of the GDPR for FB-I's contention that having "*decisive influence*" should be equated, in a GDPR context, with having responsibility as a controller for data processing activities and related decision-making about personal data.

(3) A presumption of decisive influence cannot be rebutted merely by showing that a subsidiary (acting as a controller within the meaning of Article 4(7) GDPR) makes its own decisions relating to the processing of personal data, independently of its parent company. In this connection, the General Court of the EU has acknowledged that "*[o]perational independence does not, in itself, prove that a subsidiary decides upon its conduct on the market independently of its parent company. The division of tasks between subsidiaries and their parent companies and, in particular, the fact that the local management of a wholly owned subsidiary is entrusted with operational management is normal practice in large undertakings composed of a multitude of subsidiaries ultimately owned by the same holding company*."[143] The CJEU has emphasised that, in examining whether the parent company is able to exercise decisive influence over the market conduct of its subsidiary, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to its parent company and, therefore, of economic reality.[144] The fact that a subsidiary enjoys autonomy in some aspects of its commercial activities is not sufficient, by itself, to overcome the rebuttable presumption of decisive influence which arises where a subsidiary is wholly owned (or almost wholly owned) by its parent company.[145] Rather, the key consideration is whether, in view of the economic, organisational and legal links between the parent and the subsidiary, the subsidiary enjoys real autonomy with respect to its conduct on the market overall.

(4) Accordingly, the fact that FB-I acts as a controller within the meaning of Article 4(7) GDPR for the personal data of EU users of the Facebook and Instagram services does not mean that the presumption of decisive influence by its parent company, Facebook, Inc., is necessarily rebutted.

(5) FB-I has not put forward any additional evidence in its submissions that would permit me to form a contrary view to that expressed above as to exercise of decisive influence by Facebook, Inc. over FB-I's conduct on the market.

182. In the Preliminary Draft Decision, I noted that Facebook, Inc. reported a total revenue of $85.965 billion for the year ended 31 December 2020.[146] I am satisfied, notwithstanding FB-I's submissions on this issue,[147] that the relevant "*preceding financial year*" for the purposes of Article 83(5) GDPR is the financial year preceding the issuing of the final decision of the DPC in the Inquiry following the conclusion of the Article 60 procedure (or, where applicable, any reference to the Article 65 dispute resolution procedure). At the date of circulation of the Article 60 Draft, in 2021, the preceding financial year was the year ended 31 December 2020, and Facebook, Inc.'s reported total revenue of $85.965 billion for that year was taken as the provisional turnover figure for the purpose of the Article 60 Draft. Given that this Decision has been adopted in 2022, the relevant figure is $117.929

[143] Judgment of the GCEU of 11 July 2019, *Huhtamäki Oyj*, T-530/15, EU:T:2019:498, paragraph 228.
[144] Judgment of the CJEU of 11 July 2013, *Commission v. Stichting Administratiekantoor Portielje*, C-440/11 P, EU:C:2013:514, paragraphs 60 and 66.
[145] Judgment of the CJEU of 8 May 2013, *Eni v. Commission,* C-508/11, EU:C:2013:289, paragraphs 64 to 68.
[146] Press Release, 'Facebook Reports Fourth Quarter and Full Year 2020 Results' available at <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/>.
[147] FB-I's Response to the Preliminary Draft Decision (21 July 2021), Part E, paragraph 3.42 to 3.46, page 44.

billion, being the worldwide annual turnover of the undertaking concerned (i.e. the Meta Platforms, Inc. group of companies) for the financial year ending 31 December 2021[148].

View as to the appropriate range for the administrative fine

183. In light of all of the above, and, in particular, having had due regard to each of the criteria outlined in Articles 83(2)(a) to (k) GDPR, I have decided that the appropriate range for the administrative fine to be ordered in respect of the infringement of Article 5(2) GDPR identified in this Decision would be an amount not less than €9 million and not more than €17 million. I am of the opinion that this range is appropriate, taking particular account of my view that the infringement is at the mid point of scale of potential gravity for an infringement of this nature and taking further account of the aggravating and mitigating factors, which I assessed as follows:

    a. the negligent character of the infringement, as an aggravating factor of medium weight;

    b. FB-I's decision to arrange for the Expert Review to be undertaken and the information provided during the course of Inquiry concerning the changes and improvements that FB-I made to its technical and organisational security measures following the commencement of the Inquiry, as a mitigating factor of significant weight; and

    c. FB-I's failure to do 'what it could be expected to do', for the purpose of Article 83(2)(d), as an aggravating factor of significant weight. I note, in this regard, that FB-I has submitted[149] that the DPC "appears to have already taken [this failure] into account" in the context of the assessment of whether the infringement might be characterised as negligent or intentional, for the purpose of Article 83(2)(b). I disagree that this is the case. There is, as suggested by the Article 29 Working Party guidance that has been quoted as part of each assessment, a natural overlap between the assessments that are required to be carried out for the purposes of Articles 83(2)(b) and 83(2)(d). It should be clear, however, from the assessments that have been separately recorded, above, that there are differences in the factors that have been taken into account by the DPC under each heading. In the context of the Article 83(2)(b) assessment, my focus was on FB-I's state of knowledge, as regards its obligation to implement sufficient measures to enable it to demonstrate compliance. This should be evident from the particular extract from FB-I's Response to the Preliminary Draft Decision that I included within the text of paragraph 155. The extract quoted is clearly focused on FB-I's state of knowledge and I included it as part of the Article 83(2)(b) assessment because this was precisely what was being assessed under this heading. The Article 83(2)(d) assessment, however, focused on what might reasonably have been expected of FB-I, taking into account the scale and complexity of the processing associated with the Facebook and Instagram services.

184. For the avoidance of doubt, I have taken into account – in accordance with the approach of the EDPB[150] – the provisional turnover figure referred to in the first sentence of paragraph 182 above in my calculation of the appropriate amount of the administrative fine, and I am satisfied that a fine of this level would not exceed the 'cap' imposed by Article 83(5) GDPR for an infringement of this

[148] As confirmed to the DPC by FB-I's legal representatives, by way of letter dated 14 March 2022

[149] FB-I's submissions dated 1 February 2022, entitled "Response to the [DPC's] amended draft decision received on 21 January 2022, paragraph 3.24, page 14

[150] As set out in the EDPB's binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021

nature. Having since[151] secured confirmation of the updated turnover figure, in respect of the year immediately preceding the date of this decision (i.e. the financial year ending 31 December 2021), I note that the proposed fining range remains within the permitted range, the maximum limit of which is set by Article 83(5) GDPR. I am also satisfied that an administrative fine of this range would satisfy the requirement in Article 83(1) GDPR for any administrative fine imposed to be effective, proportionate and dissuasive in each individual case. In this regard, I have taken account of:

a. The purpose of the fine, which is to sanction the infringement of Article 5(2) that was found to have occurred and to re-establish compliance with the GDPR. The fact that FB-I, from the outset of this Inquiry, took steps to commission an Expert Report and subsequently implemented, on a voluntary basis, a series of changes and improvements arising from that Expert Report is very significant, in this regard. As noted above, those changes and improvements were such that it was no longer necessary for me to proceed with the making of the order to bring processing into compliance that was originally envisaged by the Preliminary Draft Decision. I am, therefore, satisfied that the proposed fine is proportionate to the circumstances in that it does not exceed what is necessary to enforce compliance with the GDPR;

b. The circumstances of the case, which concern inadequacy in the context of having sufficient measures in place such as would have enabled FB-I to demonstrate how it applied its security measures in practice (i.e. in the context of the 12 Breaches). While the failing, in this regard, concerned the demonstration of security measures in practice, the absence of the required evidence not only infringed the accountability principle, it also hampered the DPC, in terms of its ability to assess the effectiveness of the underlying security measures. As already noted, however, it is not the case that FB-I was unable to furnish *any* of the required documentary evidence; rather, FB-I was unable to furnish *sufficient* documentary evidence. I am therefore satisfied that the proposed fine will be effective, in terms of reflecting the circumstances of this particular case;

c. The requirement for a genuinely deterrent effect, in terms of discouraging both FB-I and others from committing the same infringement in the future. As noted above, FB-I has already taken some steps towards achieving compliance with the deficiency identified by this Decision. That being the case, it is unclear how the fine proposed will not achieve the required deterrent effect; and

d. The requirement for any fine to reflect the gravity of the infringement, taking into account all the elements that may lead to an increase (aggravating factors) or decrease (mitigating factors) of the initial assessment. I have already outlined, above, how I consider the proposed fine to reflect the individual circumstances of this Inquiry.

SUMMARY OF OUTCOME

185. By way of summary of the outcome of this Decision, the corrective power to be exercised is an administrative fine pursuant to Article 58(2)(i) and Article 83 GDPR in respect of FB-I's infringement of Article 5(2) GDPR, in the amount of €17 million. In having selected this figure from the upper end of the fining range that was proposed by way of the Preliminary Draft Decision (and repeated in both the Article 60 Draft and the Amended Article 60 Draft), I have taken account of the following:

[151] As already noted, the Article 60 Draft was circulated to the CSAs on 18 August 2021

a. My assessment of the individual circumstances of this particular inquiry, as summarised in paragraphs 183 and 184, above;

b. The requirement, set out in Article 83(1) GDPR, for fines to be "effective, proportionate and dissuasive" in each individual case;

c. The views expressed by the supervisory authorities of Hamburg, Poland and Hungary during the Article 60 process, 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, taking into account the turnover of the undertaking concerned. It is important to note, in this regard, that the cooperation mechanism outlined in Article 60 GDPR requires the lead supervisory authority (in this case, the DPC) to take due account of the views that might be expressed by a CSA, further to the circulation of a draft decision. This is clear from the text of Article 60(3) GDPR. For the avoidance of doubt, I did not take into account any aspect of those views that were premised on the inclusion of additional findings of infringement, beyond those established in this Decision, or unpublished EDPB guidelines in relation to administrative fines; and

d. The views expressed by FB-I in the Response to the Preliminary Draft Decision and its further submissions of 1 February 2022[152]. While I note that those further submissions restated FB-I's position that turnover is only relevant to the calculation of the maximum fining 'cap', the EDPB determined otherwise in its decision 1/2021[153], which is binding upon the Commission. Accordingly, I am required to take account of the turnover of the undertaking when assessing the fine to be imposed in any case. I note, in this regard, the increase in turnover, as between the financial year ending 31 December 2020 (which formed the basis for my original assessment set out in the Preliminary Draft Decision and repeated in the Article 60 Draft and Amended Article 60 Draft) and the financial year ending 31 December 2021 (which, as set out in paragraph 182, above, is the relevant "preceding financial year" for the purpose of this Decision).

186. FB-I has the right of an effective remedy as against this Decision, the details of which have been provided separately.

[152] These submissions were furnished in response to: (i) the amendments that were proposed to be made to the Article 60 Draft, as well as (ii) the views that were expressed by the supervisory authorities of Hamburg, Poland and Hungary on the quantum of the proposed fine.

[153] EDPB binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021

<u>This Decision is addressed to</u>:

Meta Platforms Ireland Limited
4 Grand Canal Square
Grand Canal Harbour
Dublin 2

Dated the 15th day of March 2022

Decision-Maker for the Commission:

_____

Helen Dixon
Commissioner for Data Protection

SCHEDULE 1

Breach 1 This concerned the Facebook platform. A software bug in [redacted]s, discovered on 29 May 2018 [redacted]) caused the deletion of [redacted]' in a [redacted]database, with the consequences that: (i) during the time the bug was live, a blocked user may have been able to see the posts of an impacted user if that post was Public, 'Friends of Friends,' or in a shared space like a Group or Page, and (ii) during the time [redacted] were deleted, a previously blocked user of the Messenger facility may have been able to message an impacted user. Facebook, Inc. reversed the actions done by [redacted] and restored [redacted]' to normal settings on 5 June 2018. Communications were made (voluntarily) to all potentially affected users of the impacted platforms (e.g. Facebook and Messenger) globally by Facebook, Inc. (for and on behalf of FB-I in relation to EU Users), commencing on 2 July 2018, using in-product 'jewel' notifications.

Breach 2 This concerned unreleased alpha/beta versions[154] of the Instagram mobile application for Android. A software bug discovered [redacted] had the result that, when a user was logged in to more than one Instagram account ('Account A' and 'Account B') on a single mobile device (or shared a device with another Instagram user that was also logged into an Instagram account on the same device) and the user posted an Instagram Story or posted content to an Instagram profile during the (up to) 4 day period when the bug was live, the Story or post may have been *erroneously* published by Account A when it was *intended* to be published on Account B. The issue was resolved by [redacted] Communications were made (voluntarily) to affected users globally by Facebook, Inc. (for and on behalf of FB-I in relation to EU Users) on a phased basis, commencing on 13 July 2018, by email or (where unavailable) SMS.

Breach 3 This concerned the [redacted]. Breach 3 is particularly complex and was the subject of a series of updates by FB-I to the DPC throughout the Inquiry. In very general overview, the breach relates to software bugs first detected by Facebook, Inc. on [redacted]). Facebook, Inc.'s investigation of the issue established that, in multiple different scenarios, coding errors resulted in the unintended disclosure of the identity of a Page Admin (a user who has rights to create and edit posts on behalf of a Page), in that Page Admin names are made visible when interacting with Events, Groups or Page-posted media. Ordinarily, actions by Page Admins are attributed to, and displayed as, actions by the Page (as opposed to any individual user). The updates provided by FB-I identified a very wide variety of instances where incidents exhibiting these features occurred. FB-I indicated that [redacted] as at the date of the most recent update in respect of Breach 3 dated 24 January 2020. No notifications were made to affected users.

---

[154] FB-I explains that alpha or beta versions of the Instagram application for Android refers to "*versions of the Instagram application regularly distributed in pre-launch states to a select group of people for the specific purpose of testing functionality, stability, and other issues*" (Cross-Border Breach Notification Form for Breach 2 dated 16 June 2018, Section 3.3).

Breach 4 This concerned the [redacted] and relates to [redacted]. A software bug was discovered on [redacted]). For a period of [redacted]s between [redacted]. The issue was resolved by [redacted]. No notifications were made to affected users.

Breach 5 This affected users of [redacted] A software bug [redacted] caused [redacted]. The issue was resolved on [redacted]). The bug was live for approximately [redacted] and was fixed so that [redacted]. No communications were made to affected users.

Breach 6 This concerned [redacted]. A software bug [redacted] caused [redacted] Facebook, Inc. informed FB-I that [redacted] No communications were made to affected users.

Breach 7 This concerned posting of Facebook Live videos.[155] Facebook Live videos posted to Newsfeed are automatically cross-posted to Stories unless the user opts out of cross-posting. Facebook Stories expire after 24 hours. Posts to Newsfeed remain on Newsfeed until deleted by the user. Due to a software bug, when the cross-posted Facebook Live video in Stories expired after 24 hours, the corresponding Facebook Live video on Newsfeed was also deleted. The issue was discovered by Facebook, Inc. on [redacted] and was remediated on [redacted] Facebook, Inc. made efforts to recover those Facebook Live videos which had been inadvertently deleted, but were recoverable, and those efforts were completed on [redacted] Certain videos were permanently deleted and could not be restored. Communications were made (voluntarily) to affected users (including EU users) by Facebook, Inc. commencing on 10 October 2018, via an in-product communication.

[155] This refers to a Facebook feature which permits users to broadcast real-time video content from a Facebook profile, Page, Group, or Event which can be watched by other users.

Breach 8 This related to [redacted] Usually, [redacted] Due to a software bug, [redacted] The issue was reported to Facebook, Inc. on [redacted] and had been remediated by [redacted] No communications were made to affected users.

Breach 9 This related to [redacted]. Due to a software bug, in limited circumstances, [redacted]. This bug only happened if a set of specific conditions were met, including: [redacted] The bug did not result [redacted] The incident was reported to Facebook, Inc. on [redacted] and remediated by [redacted] No communications were made to affected users.

Breach 10 This relates to the Facebook Photo API (application programming interface). When using Facebook Login to log into a third-party app, some third-party apps give users an option to share Facebook photos with that third-party app via the Facebook Photo API. Between 13 September 2018 and 25 September 2018, a software bug affected the photo sharing functionality which is available when using Facebook Login. Ordinarily, if a user chooses to share their Facebook photos with a third-party app in this manner, the third-party app would only be able to access photos the user uploaded to their Timeline and photos the user is tagged in. The software bug led to additional photo types on Facebook being accessible by third-party apps who had received permission from Facebook users to access their Facebook photos while the bug occurred. This included: (i) photos contained in Stories (active and archived Stories), (ii) feedback reporting flow photos (when a user attaches an image to a bug they report); Marketplace photos (public photos of items for sale), (iii) temporary photos uploaded prior to their being published (stored temporarily to facilitate better posting reliability on Facebook), (iv) Facebook Groups (where the apps separately had permission to access groups photos). Photos shared in private messages were not made accessible. Nor were photos that users uploaded to Facebook with an audience choice of 'only me' or 'Custom Friends'. The issue was [redacted] and a fix for the issue became operational on [redacted] Facebook, Inc. requested third-party app developers who were potentially involved to delete all photos unintentionally acquired in this manner by [redacted] Communications were made (voluntarily) to affected users by Facebook, Inc. commencing on 17 December 2018 using an in-product jewel communication and Help Centre article. A blog targeted at developers entitled 'Notifying our Developer

Ecosystem about a Photo API Bug' was published on 14 December 2018.[156] Separate communications were made to all developers who were potentially involved via a "jewel" communication, email and a developer alert on the app's dashboard.

Breach 11 This concerned the Instagram platform. A software bug introduced by a code-change resulted in [redacted] This resulted in a [redacted], which caused certain private Instagram accounts becoming public. The software bug was discovered by Facebook, Inc. on [redacted] Communications were made (voluntarily) to affected users (including EU users) commencing on 3 January 2019 by email, SMS and webpage.

Breach 12 This affected Facebook, Facebook Messenger, and Instagram. During three specific time windows on [redacted] November 2018, a Facebook server was misconfigured and did not give effect to certain users' choices to block another user on Facebook, Facebook Messenger and Instagram. The failure of the blocking action would not have been apparent to the user immediately, but would have become apparent when the user reloaded the relevant page. Facebook, Inc. detected the issue on [redacted] Remediation measures were completed for Facebook and Facebook Messenger on [redacted] and for Instagram on [redacted] Communications were made (voluntarily) to affected users (including EU users) commencing on 20 December 2018 by in-product notification, email and SMS.

[156] Available at: https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/.