In the matter of the General Data Protection Regulation

Data Protection Commission Reference: IN-21-4-2

In the matter of Meta Platforms Ireland Ltd.
(Formerly Facebook Ireland Ltd.)

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

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

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon

____

Commissioner for Data Protection

Dated the 25 November 2022

An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

TABLE OF CONTENTS

A. INTRODUCTION

1. This is the decision (**'the Decision'**) of the Data Protection Commission (**'the DPC'**) in accordance with section 111 of the Data Protection Act 2018 (**'the 2018 Act'**) in relation to Meta Platforms Ireland Ltd ('**MPIL**') (formerly Facebook Ireland Ltd). I have made this Decision having considered the information obtained in the own volition inquiry (**'the Inquiry'**) commenced on 14 April 2021 by the Inquiry Commencement Notice ('**the Commencement Notice**'),[1] pursuant to section 110 of the 2018 Act.

2. 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 MPIL, 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 MPIL 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.[2]

B. LEGAL FRAMEWORK FOR THE INQUIRY AND THE DECISION

B.1 Legal Basis for the Inquiry

3. The GDPR is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on foot of a complaint, or of its own volition.

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

[1] Appendix D.2a.

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

B.2 Data Controller

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. MPIL had confirmed to the DPC previously by email dated 25 May 2018 that it was the controller for the Facebook service in the EU. It is understood that MPIL is also the controller for the provision of the Facebook services to users in the other EEA states (Norway, Liechtenstein and Iceland).

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. MPIL 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. In this regard, MPIL has outlined that Facebook, Inc. processes the personal data of EU users of the Facebook services on MPIL's behalf, as a processor.[3]

7. Chapter VI, Section 2 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.*

8. 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.*

9. Having considered MPIL's submissions, the Facebook Data Policy,[4] and the nature of the processing at issue, I am satisfied that MPIL is a controller (within the meaning of Article 4(7) GDPR) with regard to the processing which is the subject of this Inquiry.

[3] Appendix D.3b at 14.

[4] Appendix D.7j.

10. I am further satisfied that MPIL has its main establishment in Ireland for the purposes of the GDPR. As such, the DPC is satisfied that the requirements of Article 56 GDPR were met in relation to the processing at issue, and that the DPC must act as lead supervisory authority in respect of this Inquiry, pursuant to Articles 56 and 60 GDPR.

B.3 Legal Basis for the Decision

11. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry and any other materials which I consider to be relevant, in the course of the decision-making process.

12. On 14 April 2021, the DPC issued an Inquiry Commencement Notice, which contained details of the incident which would be the subject of the Inquiry, as well as setting out the manner in which the inquiry would proceed. The DPC provided MPIL with an Inquiry Issues Paper in order to make submissions on it on 10 December 2021. MPIL made submissions on the Inquiry Issues Paper on 21 January 2022. A full schedule of all documentation considered by me for the purpose of the preparation of this Decision is appended hereto.

13. On 24 May 2022, a Preliminary Draft Decision was provided to MPIL. This identified provisional infringements and set out envisaged corrective measures. On 14 July 2022, MPIL responded making various submissions on the matters contained in the Preliminary Draft Decision as well as providing a report [redacted].[5] In this response, MPIL disclosed, primarily within footnotes that were not elaborated upon, that it had made a number of errors across a number of its submissions. MPIL stated that due to a "*misunderstanding by the team preparing the response*" submissions erroneously referred to Messenger Contact Importer rather than Messenger Contact Creator.

14. As a direct result of this, following the Preliminary Draft Decision, in order that MPIL was afforded an opportunity to explain how the errors arose and what the extent of the errors were – as it had chosen not to do so in its response to the Preliminary Draft Decision – the DPC sent a number of queries to MPIL seeking clarity on its errors, as well as seeking amended versions of its previous submissions highlighting the errors therein. MPIL responded on 11 August 2022.

15. The DPC finalised the Preliminary Draft Decision, taking into account MPIL's submissions dated 14 July 2022 and 11 August 2022 as well as the [redacted] report. The resulting Draft Decision was circulated to the supervisory authorities concerned ('**CSAs**', each one being a '**CSA**')[6] on 30 September 2022, for their views, in accordance with Article 60(3) GDPR. Given that the matters under examination in the within inquiry entail cross-

[5] Appendix D.11c and D.11d respectively.

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

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. None of the CSAs raised objections to the Draft Decision. Comments were received from the following CSAs:

a. The Dutch SA exchanged a comment on 27 October 2022;

b. The French SA exchanged a comment on 28 October 2022;

c. The Belgian SA exchanged a comment on 28 October 2022; and

d. The Polish SA exchanged a comment on 28 October 2022.

16. As per Article 60(6) GDPR, *where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within* four weeks *after having been consulted, both the lead supervisory authority and the supervisory authorities concerned* ***shall be deemed to be in agreement with that draft decision and shall be bound by it***.

17. Accordingly, this Decision reflects no amendments to the positions or findings proposed in the Draft Decision.

C. FACTUAL BACKGROUND

18. In April 2021, media reports highlighted that a collated dataset of Facebook user personal data had been made available on the internet. This dataset was reported to contain personal data relating to approximately 533 million Facebook users worldwide (**'the scraped dataset'**).[7]

19. Accordingly, the DPC considered it appropriate to determine whether MPIL had complied with its obligations, as data controller, in connection with the processing of personal data of its users by means of the Facebook Search, Facebook Contact Importer, Messenger Contact Importer and Instagram Contact Importer features of its service, or whether any provision(s) of the GDPR and/or the 2018 Act had been, and/or were being, infringed by MPIL in this respect. Therefore, the DPC decided to commence an Inquiry under, and in accordance with, section 110(1) of the 2018 Act.

20. The Commencement Notice subsequently issued by the DPC to MPIL contained details of the incident that would be the subject of the Inquiry. It also contained queries seeking further information from MPIL in relation to the circumstances of the incident. In the course of the Inquiry, the DPC sought and received further submissions from MPIL.

21. MPIL informed the DPC that its search and contact import functionality were designed to enable people to find their friends by entering their phone numbers or email

[7] See, *inter alia*, 'Facebook data leak: details from 533 million users found on website for hackers' (*The Guardian*, 5 April 2021), accessible via https://www.theguardian.com/technology/2021/apr/03/500-million-facebook-users-website-hackers and Aaron Holmes, ' 533 million Facebook users' phone numbers and personal data have been leaked online' (*Business Insider*, 3 April 2021) accessible via https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T.

addresses—a feature that is especially useful in countries where large numbers of people share the same or similar names.

22. MPIL outlined that these features have

> *always been subject to privacy settings that allow users to restrict who can look them up and was* [redacted] *These limits make phone enumeration scraping through the search feature more difficult, but did not end it. All data returned by the phone number lookups run by scrapers was information shared publicly on Facebook. Moreover, scrapers were only able to retrieve public data for individuals whose accounts allowed phone number searches by 'everyone'.*[8]

23. MPIL contended that all data returned by the phone number lookups run by scrapers[9] was information shared publicly on Facebook and, moreover, "*…the Scraped Data Set contains information only for users whose searchability settings allowed 'Everyone' to search for them by phone number*."[10] However, as set out further below, MPIL implemented separate controls to enable Facebook users to indicate whether they wished to share their phone numbers and email addresses publicly on their Facebook profiles. The searchability features sought to enable users who already had another user's phone number or email address to use that phone number or email address to find that person's Facebook profile.

24. As described by MPIL, "*Numbers provided **solely** for 2-FA purposes were not made available for searchability (i.e. contact-matching) purposes, which prevented such phone numbers from being used to generate matches in any of the Messenger Search, Messenger CI, Facebook Search or Facebook CI features.*"[11] [emphasis added]

25. MPIL described that it has a feature called 'Contact Importer' that uses a user's submitted address book to find people they know who also use Facebook. The Contact importer enabled third parties to 'scrape' Facebook by enumerating batches of possible phone numbers from more than 100 countries, submitting them to the Contact Importer tool, and utilising it to return the names and Facebook User IDs ('**UIDs**'), which permitted a search on those UIDs to obtain any public data that users had posted on their profiles. MPIL outlined that it allowed each user to set their phone number '**audience**' and email address '**audience**' to be publicly accessible or to be limited to a restricted audience. It also has an entirely separate '**searchability'** setting, currently called '*How people find and contact you*'. That latter setting dictates whether someone can find that user on Facebook, using that user's phone number or email address through a Contact Importer feature. Even if that user's phone number had a restricted audience on their profile, it could still be publicly searchable under the setting in the

[8] Appendix D.1b at 2.

[9] Appendix D.4e: The mission in the Scraping [redacted] *"is to stop systemic extraction of user data through deliberately exposed functionality."*

Appendix D.7g: *Scraping is the automated collection of data from a website or app and can be both authorized and unauthorized. … Using automation to get data from Facebook without our permission is a violation of our terms*.

[10] Appendix D.3b at 11.

[11] Appendix D.3b at 16.

'*How people find and contact you*' feature.[12] Software providing a similar Contact Importer feature is used in the Facebook service, in Instagram and in Facebook Messenger.

26. The 'searchability' setting on the '***How do I control who can look me up***' panel defaulted to allowing every other Facebook user to run the Contact Importer and find that user's details. The same panel notes that "*you control who can see your mobile phone number or email on your profile separately…*"[13] Therefore, the switch to block Contact Importer from finding the telephone number is not the same as the switch to make a telephone number on a user profile non-public.

27. In March 2018, MPIL identified evidence of phone number enumeration scraping. MPIL described that it has in place prevention systems to slow down the ability of bad actors to be in a position to scrape information from its platforms. It sets rate limits to restrict the volume of information that bad actors can scrape in one attempt. MPIL indicated that the rate limits were reduced in both 2018 and 2019. In 2019, it created and tasked the 'External Data Misuse Team' to look into ways of preventing further scraping and utilised 'red teams' to act as bad actors. In late 2019, MPIL changed the functionality on the Contact Importer which led to the tool returning a selection of profile near matches that were not an exact match to the original phone number or email address inputted.

28. MPIL outlined that scrapers were identified in August 2019 that were using automated programmes for phone number enumeration to scrape public information via the Messenger Contact Importer. Through this activity, the scrapers were able to access a large number of user profiles and obtain a limited set of information about those users while staying beneath Messenger's rate limits.

29. MPIL made a submission on 13 May 2021 that included:

> *Third-party threat intelligence analysts were engaged to analyse the Scraped Data Set. (Neither FIL nor its processor Facebook, Inc. therefore possesses a copy of the data set.) The data set is divided into different files, by country. The analysts calculated the number of unique users within this record count by counting every unique Facebook UID contained within each file in the data set. In other words, if a Facebook UID was repeated in a country file, it was only counted once. This analysis yielded a total of approximately* [redacted] *(Some phone numbers may have been assigned to different users at different times.)*[14]

30. MPIL made a further submission on 11 August 2021 that included:

> *…the Third-Party Analyst has provided FB Inc. with a version of the Scraped Data Set in which the data values, including the UIDs, have been hashed. FB Inc. has, on*

[12] Appendix D.3b at 11.

[13] Appendix D.3b at 22.

[14] Appendix D.3b at 13-14.

> *behalf of FIL in respect of EU users, compared these hashed UIDs to hashes of UIDs in the Facebook user database, in order to look for any matches. Based on this methodology, FB Inc. has confirmed that approximately* [redacted] *valid UIDs (i.e. those UIDs that Facebook can hash-to-hash match) are contained in the Scraped Data Set. Because FB Inc. lacks a hash-to-hash UID match for the remaining approximately* [redacted] *users in the Scraped Data Set, FB Inc. cannot confirm with certainty that they are for Facebook users.*[15]

31. MPIL made a submission on 11 August 2021 that included:

> *…since the Scraped Data Set was initially obtained in April 2021, further analysis has been done on the Scraped Data Set that provides additional support for the conclusion that it derives from scraping. In particular, the analysis to date indicates that all users in the Scraped Data Set had their phone searchability setting set to "Everyone" at some point prior to the end of the Relevant Period, when it was possible for the users' accounts to be subjected to phone number enumeration scraping. … Specifically, the EDM Team has examined a random sample of 2,000 UIDs within the Scraped Data Set … and confirmed that every one of the corresponding users had their phone searchability setting set to "Everyone" at some point during the Relevant Period. This uniformity strongly suggests that the users in the Scraped Data Set were targeted through phone number enumeration scraping.*[16]

32. MPIL submitted that it only carried out detailed analysis on a sample of 2,000 records from among the [redacted] records in the scraped dataset that has been shown to have a valid Facebook UID. MPIL has failed to identify [redacted] in the dataset where the hash of the UID field failed to match the hash of any valid Facebook UID.

33. MPIL made a submission on 20 October 2021 to inform the DPC that:[17]

> *As a result of further investigation by the EDM Enforcement Team, FIL and its processor, Facebook, Inc. believes that at least one individual responsible for scraping data through Messenger Contact Importer prior to September 2019 is ***************, a Ukrainian resident. Please note that in the course of the investigations, no direct link was found between Mr ************** and the EU. Facebook, Inc. (as the contracting entity for users in the Ukraine) will be filing a complaint against Mr. ************** in the Northern District of California on 21 October 2021. The complaint will allege, among other things, that, between January 2018 and September 2019, Mr. ************** scraped publicly-accessible user data using a technique known as phone number enumeration, in violation of Facebook's Terms of Service and Platform Terms.*[1] *The complaint will seek a permanent injunction barring Mr. ************** from using services operated by the Facebook Group and will also seek monetary damages to be determined by the Court (remediation costs)…*

[15] Appendix D.4c at 8.

[16] Appendix D.4c at 5.

[17] Appendix D.6a.

> [1] *Based on the investigation to date, we do not believe that Mr. ************** was responsible for sharing the Scraped Data Set on Raid Forums, the activity which led to the publication of the Business Insider article on 3 April 2021 and generated widespread media interest in the Scraped Data Set.*

34. In its submissions of 14 July 2022, MPIL stated that "[*b*]*y the end of the Temporal Scope, all of the Relevant Features were altered so as to eliminate the ability to find specific contacts by phone number (or email address) altogether".*[18]

D. SCOPE OF THE INQUIRY

D.1 Temporal Scope

35. The Commencement Notice outlined that the scope of the Inquiry would examine and assess whether or not MPIL had complied with its obligations, as data controller, in relation to the processing of the personal data of its users, in order to determine whether or not any provision(s) of the 2018 Act and/or GDPR have been contravened by MPIL in that context.

36. The Commencement Notice and later a Supplemental Notice outlined that the Inquiry would involve an examination and assessment of Facebook Search, Facebook Messenger Contact Importer and Instagram Contact Importer.

37. The material issues in this inquiry concern Data Protection by Design and Default. Therefore, the questions to be answered in this Decision will cover the implementation of technical and organisational measures pursuant to Article 25 GDPR during the period between 25 May 2018 and September 2019 ('**the Temporal Scope**').[19] This includes regard for the features' design, evolution, engineering and deployment, given that prior to and during this time, Facebook had clearly identified instances of mass scraping with related bot and fake account activity across multiple products or features.

D.2 Material Scope

38. As initially set out in the DPC Statement of Issues, this Decision considers the application of Article 25 GDPR and the effectiveness and integration of the technical and organisational measures designed and implemented with respect to, *inter alia*, the Search and Contact importer rate limiting, other engineering tools and the fact that such features were available to be exploited by fake accounts and bots during the Temporal Scope.

39. As set out above, at the outset, the DPC considered it appropriate to determine whether MPIL had complied with its obligations, as data controller, in connection with the processing of personal data of its users by means of the Facebook Search, Facebook

[18] Appendix D.11c at [6.2].

[19] Also referred to by MPIL as 'the relevant period'.

Contact Importer, Messenger Contact Importer and Instagram Contact Importer features.

40. In its submissions of 14 July 2022, MPIL submitted that "*the ability to search for users by phone number was eliminated from the Facebook Search feature and Messenger web application in April 2018*",[20] and that "*Instagram Contact Importer is Outside the Scope of the Inquiry*", as "*the scraped data set does not include any data fields unique to Instagram, nor is there any reason to believe that any Instagram features were used to compile the scraped data set*."[21]

41. As Facebook Search was eliminated prior to the Temporal Scope, I accept MPIL's submission that it must be excluded.

42. I am not satisfied to exclude Instagram Contact Importer from the scope of the inquiry. I am not convinced that the MPIL's analysis of the dataset was sufficient to eliminate Instagram from the potential sources of the data, on the basis that MPIL's submissions state that only 2,000 records were examined in detail out of 533 million records, and that the primary method of identifying MPIL records was to see if a match of the hashed Facebook UID on the dataset existed in its own database. That method failed to match [redacted] on the dataset – some of which may have been Instagram users.[22] Per the pre-inquiry correspondence of 9 April 2021, MPIL also stated that changes were made to Instagram Contact Importer in September 2019 so that it no longer returned profiles that matched specific user phone numbers uploaded from a phone book. Such changes seem to suggest that MPIL also had concerns in relation to the Instagram Contact Importer.[23]

43. MPIL has submitted too that Messenger Contact Creator, a variant of Messenger Search, should fall within the scope of the inquiry.[24] Given the submissions regarding scraping on it, I am satisfied that this feature does fall within the scope of the Inquiry.[25]

44. Accordingly, for the purposes of the inquiry, the material scope will include Facebook Contact Importer, Messenger Contact Importer, Instagram Contact Importer and Messenger Search and its variant Messenger Contact Creator features (hereafter referred to collectively as **'the Relevant Features'**).[26]

E. ISSUES FOR DETERMINATION

45. The DPC Statement of Issues included, as matters for determination, an assessment of whether MPIL has complied with its obligations under Article 25 GDPR, which concerns the principles of Data Protection by Design and by Default.

[20] Appendix D.11c at [3.7]

[21] Appendix D.11c at [2.3], [3.7] and [3.11].

[22] Appendix D.4c at 8 and 25.

[23] Appendix D.1b at page 3.

[24] Appendix D.11c at [2.3] and [6.2 – 6.3].

[25] Appendix D.11c.

[26] The Contact Importers are variously referred to as 'Facebook CI', 'Instagram CI' and 'Messenger CI' in the various submissions.

46. This assessment involves consideration in this Decision of whether MPIL failed to comply with Article 25(1) and/or 25(2) in relation to the effectiveness and integration of the technical and organisational measures implemented during the Temporal Scope. This assessment includes regard for this feature's design, evolution, engineering and deployment, given that prior to and during this time, MPIL had clearly identified instances of mass scraping with related bot and fake account activity in the Relevant Features. This assessment includes the effectiveness and integration of the technical and organisational measures designed and implemented with respect to the Relevant Features during the Temporal Scope.

47. As Article 25 does not prescribe the implementation of any specific technical and organisational measures, or safeguards, the determination of whether data protection by design and by default have respectively been achieved must consider whether the measures and safeguards implemented were appropriate having considered the specific processing at issue.

F. APPLICATION OF THE GDPR

48. Article 2(1) GDPR defines the Regulation's scope as follows:

> *This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

49. Article 4(1) GDPR defines 'personal data':

> '*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

50. Article 25(1) GDPR provides for Data Protection by Design and states:

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

51. The requirement of effectiveness is a key element of Article 25(1), as set out in the EDPB guidelines:

> *Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.*
>
> *...First, it means that Article 25 does not require the implementation of any specific technical and organisational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk. Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing.*
>
> *...Second, controllers should be able to demonstrate that the principles have been maintained.*[27]

52. Article 25(2) provides for Data Protection by Default and states

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

53. The EDPB has published Guidelines on Data Protection by Design and by Default, which summarise Article 25 as follows:

> *The core of the provision is to ensure appropriate and effective data protection both by design and by default, which means that controllers should be able to demonstrate that they have the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.*[28]

54. Recital 78 is also relevant. It states:

[27] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, subchapter 2.1.2.

[28] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default at [2].

> *The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default· Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.*

G. ASSESSMENT OF CERTAIN MATTERS CONCERNING ARTICLE 25 GDPR

55. This Decision concerns MPIL's processing of users' personal data in the Relevant Features. As outlined above, these features were designed to enable people to find profiles of people known to them by entering their phone numbers or email addresses.

56. The assessment of MPIL's compliance with Article 25(1) and (2) must have regard to the nature, scope, context and purposes of this processing and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing in the Relevant Features. In assessing MPIL's compliance with Article 25(1) and (2), I must also take into account the state of the art of the cost of implementation.

57. In its submissions of 21 January 2022, MPIL stated:

> *The Relevant Features through which phone number enumeration scraping is believed to have been conducted during the temporal scope of the Inquiry are Facebook CI, Messenger Contact Importer ("Messenger CI") and Messenger Search for mobile devices. These features, including their phone number-lookup functionalities, provided significant benefits to users, which must be considered as part of the nature, context, and purpose of the processing.*
>
> *Facebook CI and Messenger CI offer a user the ability to upload their mobile phone address book/contacts in order to help the user connect with those contacts on Facebook or Messenger. For example, suppose Jane is a new user of Facebook and wants to connect with people in her address book who already use Facebook. She can use Facebook CI to upload the names and numbers of the people in her mobile phone address book so that Meta Ireland can check whether or not any are existing users of Facebook. During the temporal scope, a function would be run on*

> *the data to evaluate which uploaded phone numbers, if any, were associated with other Facebook users. Subject to the searchability settings of the relevant users (as well as other controls, as described further below), a list of users would be provided to Jane, who could then reach out to these contacts to connect on Facebook or Messenger.*
>
> *Similarly, Messenger Search on the mobile app is a central function on the mobile messaging application that allows Messenger users to search for people they know on Messenger. During the temporal scope, phone number-lookup functionality included as part of the feature enabled users to type in a person's phone number and immediately see if they could send a message to the person, similar to the experience of sending an SMS message. <u>Messenger Contact Creator (which was a variant of Messenger Search) likewise enabled a user to search for an individual by phone number while also simultaneously adding them to their contacts on Messenger.</u>*
>
> *The Relevant Features served a meaningful purpose for Facebook and Messenger users during the temporal scope, by helping them to connect with friends, family, and meaningful communities - a core value of the Facebook service. Phone numbers in particular are often the main contact points that users have for other users, and thus the phone number-lookup functionalities of the Relevant Features made it especially easy for users to find their contacts on Facebook and Messenger. The Relevant Features used only data that was necessary in relation to this purpose (i.e., a phone number already in the possession of the searching user).*
>
> *This nature, purpose, and context of the processing is important to consider as part of the Article 25 analysis. Given the significant benefits provided by the Relevant Features, any efforts to prevent the use of the features by scrapers had to be balanced against the need to allow use of these beneficial features by ordinary users. This is what makes anti-scraping efforts so challenging: the functionalities abused by scrapers are typically features, not bugs; and if anti-scraping controls are too restrictive, then ordinary users may lose the benefit of those functionalities.*[29]

<u>G.1 Nature of Processing</u>

58. The nature of processing refers to the basic or inherent features of the operations performed on personal data by a controller. MPIL's processing of users' personal data in the Relevant Features concerns a process whereby individuals can lookup phone numbers and email addresses and Facebook returns the names and UIDs, which

[29] Appendix D.8d at [9]-[13]. The underlined segment was added by the amendment to this submission in Appendix D.12f at [11.]

permitted a search on those UIDs to obtain any public data that users had posted on their profiles.

G.2 Scope of Processing

59. The scope of processing refers to the extent of operations performed on personal data by MPIL. This processing was limited to Facebook and Instagram users who had their searchability setting enabled to allow others to search for them via their phone number or email. However, this setting for each user was set by default to enable every other Facebook user to find them. It was open to users to change this in their settings. As set out above, MPIL identified [redacted] Facebook users in the scraped dataset from EU countries and therefore it is clear that a very large number of data subjects were searchable under the Relevant Features during the Temporal Scope. MPIL also failed to identify [redacted] in the dataset where the hash of the UID field failed to match the hash of any valid Facebook UID, so it is possible the number could indeed be higher. The processing of personal data in the Relevant Features matched phone numbers and email addresses with the names of the owners of those details and with other information from the Facebook profiles. In light of this and the number of Facebook users who were searchable under the features, I consider that the scope of the processing was broad.

G.3 Context of Processing

60. The context of processing refers to the circumstances that form the setting of the processing. While the features were designed to enable people to find the profiles of persons known to them, the context enabled strangers to enter random strings of numbers and text, and if those strings matched a Facebook user's phone number or email address, Facebook would match that number or email address to the identity of its owner and their Facebook profile. This context created a risk of scraping phone numbers and email addresses and connecting them to their owners' identities. The context of the processing also concerned a large social media platform in which all users' settings were set by default to enable every other Facebook user to find them. This context increased the risk of scraping because it meant that random numbers and emails were more likely to result in a match under the Relevant Features.

G.4 Purposes of Processing

61. The purposes of processing refers to the reasons for processing personal data. MPIL outlined that the Relevant Features were designed to enable people to find their friends by entering their phone numbers or email addresses. MPIL also outlined that this feature is especially useful in countries where large numbers of people share the same or similar names. MPIL also outlined that it is a core value of Facebook to connect people, around the world, with friends, family, and meaningful communities and that providing users with that experience often depends on their searchability settings under the relevant feature:

> *The Relevant Features enable users to locate and connect with friends, family and communities around the world – as is central to Facebook's core purpose. The phone number-lookup functionalities that were part of the Relevant Features*

> *during the temporal scope were designed for this same core purpose, as they allowed users to locate others and to be located by others based on phone number, which is often the main contact point that one user may have for another. As is often the case with scraping, any efforts to limit the potential for scraping of these features came with a corresponding trade-off of limiting the potential usefulness of these important features for ordinary users.*[30]

G.5 Risk

62. In implementing measures pursuant to Article 25 GDPR, the controller must have regard to the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

63. Recital 75 to the GDPR provides examples of risks to the rights and freedoms of natural persons. These risks may include physical, material or non-material damage to natural persons. In particular, Recital 75 specifies the following relevant risks to the rights and freedoms of natural persons:

> *The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.*

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

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

[30] Appendix D.8d at [4]. See also at [9]-[13].

65. The European Data Protection Board has stated:

> *29. The GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing).*
>
> *30. When performing the risk analysis for compliance with Articles* [sic] *25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments.*
>
> *…*
>
> *32. … controllers … must always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed. ...*[31]

66. Therefore, in complying with the requirements of Article 25, in the first instance, it is appropriate to identify the risks to the rights of data subjects that a violation of the principles presents. One must have regard to the likelihood and severity of those risks and must implement measures to effectively mitigate them.

67. In its response of 14 July 2022, MPIL made a number of submissions:

> "*aside from phone numbers, every single item of data in the Scraped Data Set was already publicly viewable on the corresponding user's Facebook profile at the time of the scraping*",[32] that "*for the majority of EU users in the Scraped Data Set, the only information besides phone number included in the data set consists of Facebook name, UID, and gender*",[33] and these submissions also addressed SIM swapping and impersonation, and the risk of physical damage, and robocalls and smishing.[34]

68. MPIL submitted a report [redacted] of 14 July 2021, set out above, which made submissions in relation to the risk posed by the infringement. [redacted] described himself as [redacted] an international cybersecurity consulting company with over 20 years of cybersecurity and cybercriminal investigation-related experience.

69. From the outset he stated:

> *I disagree with the PDD's finding that the categories of data in the Scraped Data Set "carry a risk with regard to the fundamental rights and freedoms of data*

[31] Appendix D.9b at 9-10.

[32] Appendix D.11c at [24.5].

[33] Appendix D.11c at [24.6].

[34] Appendix D.11c at [24.7]-[24.18].

subjects, in particular in relation to identity theft and fraud." Aside from phone numbers, the Scraped Data Set consists of fragmentary items of non-sensitive profile information that users had made publicly viewable on the Facebook platform at the time of the scraping. Based on my experience, such data would be of minimal use to a malicious actor seeking to commit serious forms of cybercrime such as fraud or identity theft, which typically require more extensive and sensitive information about a person (such as financial information or online credentials).[35]

I also disagree with the PDD's finding that the inclusion of phone numbers in the Scraped Data Set poses a "particularly high" risk to users because of the risk of "impersonation" through "SIM-swapping"—a scheme in which a bad actor tricks a mobile carrier into transferring a user's phone number to the criminal's own device. SIM-swapping requires far more than knowing someone else's phone number. In order to successfully take over control of a victim's phone number, a fraudster needs various types of information necessary to verify a user's identity with the phone company. Nothing in the Scraped Data Set would, in my experience, be sufficient to meet a phone carrier's requirements.[36]

I also disagree with the PDD's assertion that users face an enhanced risk of physical harm, including the risk of stalking and burglary, due to the release of "location information" in the Scraped Data Set. I understand that the only information in the Scraped Data Set relating to a user's "location" is the "current city" that was listed on users' profiles when the Scraped Data Set was compiled (in 2018 and 2019). This is not the sort of precise or current location information that would help a bad actor track a person's whereabouts and would be of little value to a would-be burglar or stalker.[37]

The PDD also finds that bad actors may use information from the Scraped Data Set for various forms of spamming users. It is true that the phone numbers included in the Scraped Data Set (like any phone numbers) could be used for spam-type phone communications – in other words, robocalls or "smishing" messages. However, robocall and smishing campaigns have been ubiquitous for years. Any increase in the risk that users in the Scraped Data Set will be targeted by these campaigns – or will fall victim to them – seems marginal.[38]

Finally, I note that the mere fact that the Scraped Data Set was published on an online forum used for selling or posting data sets does not, based on my experience, by itself imply a risk to users. It is common for data of limited to no value to criminals to be posted on these forums, especially when the data is made available for free, like the Scraped Data Set was. Commentary from more experienced actors on some of these forums specifically notes the low value of the data it contains.[39]

[35] Appendix D.11c at [4] and elaborated at [15]-[18].

[36] Appendix D.11e at [4] and elaborated at [19]-[28].

[37] Appendix D.11e at [4] and elaborated at [29]-[31].

[38] Appendix D.11e at [5] and elaborated at [23]-[36].

[39] Appendix D.11e at [5] and elaborated at [37]-[41].

70. More specifically, in relation to the his first point of disagreement, [redacted] stated:

> *Regardless of what specific data elements are included for a particular user, in my opinion the inclusion of these categories of information in the Scraped Data Set does not meaningfully increase the risk of harm to affected users, since it is profile information that was already publicly viewable on the users' Facebook profiles. To the extent any malicious actor wanted to obtain this information about a particular person included in the Scraped Data Set, they could have done so simply by going onto Facebook*. […] *In my experience, malicious actors are deeply familiar with these sites and how to access and search for information on them. Thus, whatever risks there were from the information being publicly available existed prior to the scraping of the information*
>
> *The only information included in the Scraped Data Set that was potentially not publicly viewable on the users' Facebook profiles at the time of the scraping consists of phone numbers, which I address further below. But the rest of the data in the data set is all data that was publicly viewable regardless and therefore, in my view, its inclusion in the Scraped Data Set does not present any substantial increase in risk – certainly not any "high," "severe," or "serious" risk.*[40]

71. While assessing the categories of personal data in isolation may produce a different risk profile, the risk is exacerbated by how it was possible to match these categories of personal data with the data subjects' phone numbers. Simply because some personal data is available elsewhere or on an individual Facebook profile does not, in itself, ameliorate the risk posed by the disclosure of that personal data –a very detailed profile of the data subject. Indeed, to ignore the inclusion of the matching of a data subject's phone number to the rest of their identifying personal data is itself quite artificial in the premises.

72. In relation to his second point of disagreement, [redacted] primarily asserted that the disclosed data does not include the categories of personal data required in order to SIM-swap. He stated that knowing facts like someone's name, hometown, relationship status, or even date of birth is not enough to steal someone's identity and that, for example, in order to open a bank account one would need hard identifies such as a proof of identification and proof of address.[41] He stated:

> *While I understand that a phone number was not, for many users, among the information users chose to share publicly, disclosure of a person's phone number does not, by itself, meaningfully increase the risk that a person will be the victim of criminal activity. I am not aware of any means by which a malicious actor could use a phone number, standing alone, to commit identity theft, hack into existing accounts, or perpetrate other common forms of cybercrime*.[42]

[40] Appendix D.11e at [17]-[18].

[41] Appendix D.11e at [20]-[22].

[42] Appendix D.11e at [23].

He stated that "*phone numbers are widely, and voluntarily, circulated because, in my experience, people do not view them as creating a serious risk of fraud. Those views are entirely consistent with my experience",* that more information would be required to fraudulently take over a phone account,[43] and that "*there is no known way to perpetuate SIM-swapping attacks en-masse*".[44]

73. The centrality of the phone number paired with the other categories of personal data is the basis of the high risk posed by the disclosure. While considered within the limited prism of the opening of a bank account, the risk may seem reduced, but this ignores the variety of other forms of identity theft to which a data subject may become exposed. Such forms could include using personal data to gain access to an existing account, or to contact friends and family of the data subject on the basis of their identity to defraud them. Identity theft may also arise for a variety of other purposes that may be non-financial, such as in the context of intimidation, harassment or coercion. While bad actors may prefer to spend their time seeking more sensitive personal data, that does not in itself mean that the categories of personal data disclosed are of no utility. Simply because some of the personal data are publicly available or are circulated by the data subject themselves, this does not mean there is no or minimal risk.

74. In relation to his third point, [redacted] stated:

> *In order to stalk an individual or commit a burglary based off information about the individual's location, a criminal would need more specific and current location information about the user—starting with a specific address, but also information to show an individual's whereabouts at a specific time or their specific travel patterns. However, the only "location" data potentially in the Scraped Data Set is a user's inputted "current city" —for example, Dublin, or Brussels, or London. Not only is this information likely to be available from other sources—if a criminal is seeking to stalk or burglarize some specific person they are likely to already know at least what city they live in—but merely knowing the city where a user resides does not give a stalker or a burglar enough information to go on.*[45]

He adds that such information may not be current and the data subject "may" have moved elsewhere, and that "merely" knowing someone's phone number does not provide an ability to know their whereabouts.[46]

75. In the premises, the individual data may indeed not be specifically useful to a bad actor in isolation. However, the categories of personal data provided a detailed profile of that person. Further, the extent of the personal data disclosed meant that a data subject could be targeted in the context of coercive control and domestic violence. "Merely" knowing someone else's phone number can open them to sustained harassment from a former partner and indeed can heighten the risk of physical harm.

[43] Appendix D.11e at [24]-[27].

[44] Appendix D.11e at [28].

[45] Appendix D.11e at [30].

[46] Appendix D.11e at [30]-[31].

76. With regard to [redacted] fourth point, he stated that as robocall and smishing campaigns have been ubiquitous for years, any increase in the risk that users in the Scraped Data Set will be targeted by these campaigns seems marginal.[47] He stated that he "*agree*[s] *that the phone numbers in the Scraped Data Set could be used to contact people for these purposes, but this is a risk that phone users already face generally*".[48] He further stated that the information gathered from a user's Facebook profile would not be practical or relevant to use for the smishing or robocall message,[49] that the main benefit of the Scraped Data Set for conducting robocalls and smishing is that a list of verified phone numbers reduces the incidence of calls or texts not going through due to invalid numbers,[50] that as "*people routinely receive unsolicited calls and texts already*" that "*this is a generally experienced phenomenon of modern life*".[51] He stated that there is a very low likelihood of 'spear-fishing' as this is typically targeted at corporate executives or employees with valuable access to corporate resources.[52]

77. [redacted] [redacted] accepted that there is indeed a risk of the above posed by the disclosed data set. Given the extremely large size of the data set, its risk of utilisation for these purposes is significant. While Mr [redacted] seemed primarily concerned with the content of such robocalls, the fact of the calls themselves lends to the risk. While lists of viable phone numbers may be available elsewhere, this does not mitigate or reduce the risk arising from the disclosed data simply because it is one of those viable lists. I do not accept [redacted] apparent submission that, just because persons have experienced smishing or robocall before, this somehow reduces or mitigates the risk of it happening due to the disclosure of the scraped data.

78. Fifth and finally, Mr [redacted] stated that the mere fact that the Scraped Data Set was published on an online forum used for selling or posting data sets does not by itself imply a risk to users.[53]

79. The fact of it being placed on a particular forum was not the premise of the determination of the risk in the Preliminary Draft Decision. Rather, it was the disclosure of the personal data itself and its categories. Simply because individual forum users may not have sought to utilise the personal data, is not evidence, in itself, that the disclosure of the scraped data set did not pose a risk. For all of these reasons, I do not accept Mr [redacted]' contentions.

80. MPIL has failed to demonstrate that it carried out an analysis of the risk arising from the chosen design as recommended by the EDPB Guidance quoted above. In the Supplemental Notice of 30 September 2021, MPIL was asked to provide an assessment of the identified risks during the period 25 May 2018 until September 2019 that were associated with the Relevant Features and data processing systems and services on the Facebook platform that were directly involved in the disclosure of the personal data in

[47] Appendix D.11e at [5].
[48] Appendix D.11e at [32].
[49] Appendix D.11e at [33].
[50] Appendix D.11e at [35].
[51] Appendix D.11e at [35].
[52] Appendix D.11e at [36].
[53] Appendix D.11e [37]-[41].

the dataset. MPIL was asked to include the inventory of such identified risks during this period. In response, MPIL outlined a number of measures which it put in place *"…based on assessments of risk in response to observed scraping activity…".* [54] The measures included the adjustment of rate limits, the elimination of contact matching and the establishment of a 'red team' and arose as a reaction to scraping activities. These measures are examined below.

81. However, the response failed to provide any substantive information with regard to risk assessments. MPIL had previously provided risk assessment documentation that was created by the EDM team.[55] However, this document is dated December 2020, subsequent to the period referred to in the above query. While the MPIL [redacted] of May 2019 relates to some of the temporal scope, as detailed below, this document is also subsequent to much of the temporal scope. Furthermore, the MPIL [redacted] failed to take account of, *inter alia*, the risks to the rights and freedoms of varying severity for natural persons "*at the time of the processing itself*", i.e. since 25 May 2018.

82. MPIL stated in its submissions of 21 October 2021 that

> *…there are no well-developed "industry standards" for anti-scraping controls, as there are for traditional security or privacy programs.*[56]

Given MPIL's statement there are no well-developed standards to adhere to with regard to anti-scraping measures, it brings more importance to the act of risk assessment and mitigation that should be undertaken prior to implementing that kind of measure.

83. Further, in its submissions dated 21 January 2022, MPIL stated that:

> *the basic risk from any type of scraping of Facebook surfaces is that it involves collecting data available on Facebook and thereafter potentially making it available somewhere else. This can entail a certain degree of user loss of control over the data. Meta Ireland fully recognises this risk, which is why substantial resources were, and continue to be, devoted to combating scraping.*[57]

Accordingly, while MPIL appears to accept that it recognised and was aware that scraping activities pose risk, it did not engage in any assessment of that risk relevant from the beginning of the temporal scope.

84. MPIL further stated that the "*mere occurrence*" of scraping does not imply a failure of data protection by design:

> *Article 25(1) GDPR requires the implementation of 'appropriate' measures that are 'designed' to implement data protection principles in an effective manner – not the elimination of all risk.*[58]

[54] Appendix D.7c at 2.

[55] Appendix D.4f.

[56] Appendix D.7c at 3.

[57] Appendix D.8d at [14].

[58] Appendix D.8d at 3.

While MPIL is correct to the extent that risk cannot be eliminated entirely in many instances when processing personal data, risk needs to be appropriately identified and mitigated. Where a risk has been newly assessed, or re-assessed, and that risk applies to multiple different aspects of a processing system, the same, or similar, mitigating measures should be put in place with the goal of mitigating that identified risk in all aspects of the processing where it occurs.

85. MPIL has emphasised that the technical and organisational measures in place throughout the Temporal Scope were appropriate, effective, integrated into the Relevant Features and state of the art, and that, when taking into account the nature, scope, context and purpose of the processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, full consideration must be given to the benefits of the Relevant Features to users and their importance to the core purpose of Facebook; the privacy settings that enabled users to control who could search for them by phone number or who could view information in their profiles; and the lack of any state of the art controls that provided a means to prevent scraping of the Relevant Features altogether without eliminating functionalities useful to ordinary users.[59] However, these measures, whether *pre*- or *post-hoc*, do not address the assessment and appraisal of the risks posed by scraping.

86. The earliest documented account of the relevant risks provided by MPIL was the MPIL [redacted] of May 2019.[60] It identified the more specific harms that can happen:

- *Users whose contact information is scraped could get spammed, causing inconvenience and even financial loss.*
- *Leaking health information can cause untold harms to users. Users can end up being denied employment opportunities, housing, and insurance based on their health status despite laws forbidding such discrimination. It could be catastrophic to the lives of Facebook users, as well as to the reputation of Facebook itself, if user health data were scraped. To our knowledge, there is no way of scraping health data, but making sure that's true, and that it stays true, is important.*
- *Leaking location information can also be incredibly harmful to users. They can end up in physical danger if such information ends up in the hands of stalkers. Their homes can be burglarized when they are out. And location information can end up revealing all manners of sensitive information just from the locations the user visits. Like health data, there aren't many avenues of scraping location information, but the harms that could result are substantial.*
- *Other user data, such as posts, comments, group memberships and page likes, can end up in the hands of companies like Cambridge Analytica and be used for targeted advertising and/or political campaigns. We know from experience that this represents an enormous breach of trust between us and users and must be avoided.*

[59] Appendix D.8d at 11.

[60] Appendix D.4e.

87. In its submissions of 14 July 2022, MPIL stated that "*the potential risks to users from scraping were in fact assessed within the Temporal Scope, including in a written assessment produced to the DPC as part of the Inquiry. That assessment, a* [redacted] *prepared in May 2019 specifically discussed the harms that might arise specifically as a result of contact information scraping*" and "*the PDD's preliminary conclusion is that MPIL 'did not engage in **any** assessment of [scraping] risk', and that conclusion is plainly incorrect.*"[61] The Preliminary Draft Decision drew attention to the fact that having identified a risk that was ongoing before the Temporal Scope, there was a lack of appropriate engagement to mitigate the ongoing risk in a timely manner. The May 2019 [redacted] was the first submitted document to demonstrate a detailed assessment of risk. This May 2019 [redacted] did not take account of, *inter alia*, the risks to the rights and freedoms of varying severity for natural persons "*at the time of the processing itself*", i.e. since 25 May 2018.

88. MPIL then stated that:

> *Moreover, it is evident that assessments regarding the risks relating to scraping were also made prior to the Temporal Scope, based on the modifications that were proactively made to the Relevant Features in April 2018, after scraping was discovered on the Facebook Search feature and the ability to search for users by phone on the feature was eliminated.* […]
>
> *Also in April 2018, MPIL addressed scraping via a public blog post, which highlighted the removal of the ability to search for users by phone on Facebook Search – notwithstanding the fact that search by phone had proven "especially useful for finding your friends in languages which take more effort to type out a full name, or where many people have the same name." This is further evidence that, contrary to the DPC's preliminary findings in the PDD, there was awareness of the potential risks of scraping and a willingness to take action to address such risks, even where the mitigations had the negative effect of eliminating legitimate, useful user features.* [62]

Despite, MPIL's submission that it is "*evident*" that the risk assessments were made, no documented record of them has been provided. Mitigations differ from risk assessment. Risk awareness differs from risk assessment. Doing one does not ameliorate the need to have done the other. I do not accept that a public blog noting the removal of the ability to search for users by phone on Facebook Search constitutes risk assessment.

89. I accept the specific harms listed in the [redacted] above, while noting that these harms did not specifically include the risk of fraud and impersonation as set out below, nor the risk of processing involving a large amount of personal data that affects a large number of data subjects.

90. It is clear that MPIL's processing of users' personal data in the Relevant Features presented risks relevant to a number of the data protection principles provided for in

[61] Appendix D.11c at [10.3]-[10.4].

[62] Appendix D.11c at [10.5]-[10.6].

Article 5 GDPR. In assessing MPIL's compliance with Article 25, I must have regard to the risk of bad actors misusing the Relevant Features to acquire the phone numbers and email addresses in a manner that matches these contact details to those identified users and to other personal data posted publicly on their profiles. It is clear that this risk relates to a number of data protection principles as provided in Article 5 GDPR.

91. The risk, for example, relates to the purpose limitation principle provided for in Article 5(1)(b) GDPR because of the potential that Facebook users' phone numbers, email addresses, and other personal data could be processed in a manner that is incompatible with the purposes for which the personal data were collected. The Relevant Features were designed to enable Facebook users to connect with one another. However, where the Relevant Features are used by bad actors to create a data set, rather than finding profiles of Facebook users known to them, this would amount to processing of personal data in the Relevant Features in a manner that is incompatible with the purposes for which the personal data were collected.

92. In its submissions of 14 July 2022, MPIL stated that this is a misapplication of the purpose limitation principle and that the Preliminary Draft Decision intimates that "*the third-party use of the Relevant Features for the purpose of mass-scraping is processing that is incompatible with the purpose for which MPIL collected user phone numbers from users, and that constitutes an infringement by MPIL of the purpose limitation principle*."[63]

93. The Preliminary Draft Decision does not do this. Rather, the issue is that MPIL was obliged to implement appropriate measures to implement the purpose limitation principle. The Preliminary Draft Decision is not attributing the actual use by bad actors of the Relevant Features to MPIL, rather it states that a risk arose in the utilisation of the Relevant Features in this manner to the purpose limitation principle. MPIL appear to be suggesting that an application of the purpose limitation principle which would render it pointless if data controllers had no obligations to implement appropriate organisational and technical measures where there was a risk that a bad actor could utilise features inappropriately. The Relevant Features are MPIL's features and it was through these features that the phone numbers were disclosed to the scrapers. MPIL accordingly has a responsibility under the GDPR to implement appropriate measures to prevent the features being used for a purpose other than that intended - for example confirming phone numbers, matching to other categories of personal data.

94. Further, the risk also relates to the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR. This principle requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing. Where a user's searchability setting is set to enable other users to find them, the Relevant Features are designed to enable individuals who already have that user's email address or phone number to find their profiles. These searchability settings must be distinguished from a Facebook user's decision to make their phone number or email address publicly available on their

[63] Appendix D.11c at [[9.2]. See [9.1-[9.8] in total.

Facebook account, for which Facebook implements the separate audience settings. Therefore, the Relevant Features create a risk of unauthorised access to Facebook users' phone numbers and email addresses. This could take the form of bad actors using the Relevant Features to discover whether random combinations of numbers and letters correspond to valid phone numbers and email addresses, and, if so, to discover the identity of the Facebook user who owns the relevant phone number or email address. The searchability settings seek to make users' profiles discoverable where another user already has a user's phone number or email address, but they are not intended to allow strangers to find the contact details of identifiable Facebook users, nor are they intended to allow personal data to be web scraped. Any such access to that data as a result of misuse of the Relevant Features would be unauthorised access.

95. In its submissions of 14 July 2022, MPIL also stated that the DPC misapplied the facts to the principle of integrity and confidentiality.[64] MPIL attempted to make the distinction that the scrapers did not access the phone numbers of users, rather they were input by the scrapers as part of their scraping method, and linked to users "*by inference*".[65] [redacted] MPIL appears here to be attempting to argue that by users having their privacy settings set to 'Everyone', this was the same as users consenting or permitting the Relevant Features to be utilised to scrape their phone numbers and link it to their profiles. Users have a reasonable expectation of privacy, integrity, and security. This MPIL submission is unsustainable in claiming that such scraping did not constitute a form of "*unauthorised access*".

96. The risk also relates to the data minimisation principle provided for in Article 5(1)(c) GDPR. This principle requires that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In circumstances where MPIL automatically set the Relevant Features to include each user's phone number and email address, there was potential for the Relevant Features to process personal data that was not relevant and limited to what was necessary for the specific purposes for which those phone numbers and email addresses were processed. For example, phone numbers are also used as a unique identifier in the Facebook service. However, by automatically processing such phone numbers in the Relevant Features there was potential that the processing in the Relevant Features would not be relevant and limited to what was necessary in relation to that purpose. This default setting not only made the users' accounts automatically searchable by their contact details, but also exposed those contact details to potential scraping as set out above. MPIL was under an obligation to implement appropriate measures to ensure that, by default, only personal data which are necessary for each specific purpose of the

[64] Appendix D.11c at [9.9]-[9.14].

[65] Appendix D.11c at [9.11].

processing are processed and that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

97. I consider that the likelihood of the risk presented by MPIL's processing of personal data in the Relevant Features was severe. Every Facebook user had access to the Relevant Features. Therefore, the likelihood of misuse by some individuals was significant. I have also had regard to the scope and context of the processing and how the searchability setting for each user was set by default to enable every other Facebook user to find them. This added to the likelihood of the risk of scraping because it resulted in a larger set of data against which random phone numbers and email addresses could match.

98. Phone numbers and email addresses can be targeted for fraud, impersonation and spamming. They are persistent forms of personal data, which are infrequently changed or abandoned by the holder. These contact details are frequently used as personal identifiers in the context of numerous online and offline services, posing a potential fraud risk where these personal data are utilised. Where these contact details can be linked to other personal data, such as a user's full name, the risk of fraud and impersonation increases significantly and users are placed at a heightened risk of being the victims of serious forms of fraud, including financial fraud, impersonation and loss, whether that be financial, of their personal data and/or of private and confidential information more generally. There is an overlapping risk of data subjects being potentially directly affected by the disclosure of their personal data and those who know such persons being subjected to a range of scams. Such scams can include, but are not limited to 'phishing' or 'smishing' scams whereby fraudsters leverage email addresses and phone numbers in order to trick persons into disclosing or inputting confidential passwords or codes, or where fraudsters may impersonate a data subject who has had their personal data disclosed in order to defraud others. The potential severity of consequences of individuals is plainly quite high given both the categories and the range of personal data has been disclosed.

99. The risk posed by the disclosure of phone numbers in particular is particularly high. Fraudsters can use phone numbers to engage in extensive fraud and impersonation such as 'SIM-swapping' whereby mobile carriers are tricked into transferring a data subject's phone number to a fraudster's device in order to carry out fraudulent activities, such as gaining access to bank accounts, or resetting their email and social media account credentials. This is particularly the case given that the Relevant Features match the numbers provided by scrapers to further personal data thus creating a more complete profile of the data subject that can then be used by fraudsters to trick financial institutions, among others, into believing they are the data subject.

100. Additionally, the ability to use the Relevant Features in this manner constitutes processing involving a large amount of personal data and affects a large number of data subjects. MPIL indicated that the scraped dataset contained the personal data of approximately 533 million Facebook users worldwide. The analysis submitted by MPIL identified [redacted] unique UIDs belonging to data subjects from within countries of the EU. In light of the number of data subjects affected, the large amount of personal

data and, as set out above, the very nature of that personal data, the severity of the risk for rights and freedoms of natural persons posed by the processing was high.

101. I consider that the severity of the risk for rights and freedoms of natural persons posed by the processing was high. As well as phone numbers and email addresses, the relevant personal data processed by MPIL included any public data that users had posted on their profiles and any personal data marked as public. MPIL stated:

> *By way of example, What is public information on Facebook?, published in the Facebook Help Center* […], *makes clear as follows: "Your Public Profile includes your name, gender, username and user ID (account number), profile picture, cover photo and networks. This info is also public".*[66]

102. In conclusion, I am satisfied that there are possible and severe risks associated with the processing which is the subject of this Inquiry; these risks are primarily related to fraud, impersonation and scamming. I am also satisfied that MPIL did not take adequate steps to assess and appraise the risk posed.

H. TECHNICAL AND ORGANISATIONAL MEASURES IMPLEMENTED BY MPIL

103. This Decision considers the technical and organisational measures implemented by MPIL pursuant to Article 25(1) and (2) GDPR regarding the Relevant Features during the Temporal Scope.

104. MPIL has set out its implementation of technical and organisational measures in its various submissions during the Temporal Scope. All such submissions, exhibits and documentation has been considered in full.

105. In its submissions dated 21 October 2021, MPIL made submissions specifically regarding the measures it uses to prevent scraping, stating that, broadly:

> *… is a continuous process that seeks to (i) identify actual and potential scraping vectors, and (ii) develop and refine the mitigations deployed to counter the evolving tactics and methods used by scrapers. Examples of the evolving assessment and mitigations put in place to counter scraping relevant to the Dataset during the period from 25 May 2018 include the following:*
>
> - *Rate limits were adjusted at various times based on assessments of risk in response to observed scraping activity….Rate limits remained in effect on the Relevant Features between 25 May 2018 and September 2019.*

[66] Appendix D.7c at 2-3.

- *In October 2018, the Abusive Account Detection Team discovered evidence of a large number of scripted accounts using Facebook CI. In response to the discovery of these new tactics contact matching was eliminated altogether from Facebook CI in favor of PYMK suggestions, so as to obfuscate any link between an individual user and uploaded phone number or email address thus mitigating the risk of the feature being used for scraping in light of the observed changes in scraper tactics*
- *In August 2019, the EDM Team established a "red team" that focused on identifying methods of scraping data on Facebook products and features so as to help the EDM Team improve antiscraping controls. In late July 2019, the EDM Team reported that it had found feasible methods of conducting phone number enumeration scraping on Messenger Search* [~~and Messenger CI].~~ *These findings enabled the EDM Team to discover patterns of Messenger usage consistent with the scraping method identified by the red team, indicating that scraping was likely occurring via these features on Messenger. This discovery led to a number of changes to Messenger Search and* [~~Messenger CI~~] *to reduce and deter further scraping, including eliminating the search-by- phone-number and search-by-email functionality from Messenger Search and eliminating contact matching from Messenger CI.*[67]

106. I have taken note of the timeline involved in the remedial measures established by MPIL to counteract the threat of scraping.

107. In March and April 2018, MPIL identified evidence of phone number enumeration scraping as part of an internal data science review around search reliability. The Facebook Search feature had been subject to privacy settings that allow users to restrict who can look them up and was [redacted][68]

108. MPIL stated that in March 2018, in the course of an integrity review of the Facebook Search feature, the Facebook Search team discovered anomalously high usage of Facebook Search by [redacted] It was concluded that the usage was likely scraping activity. While Facebook Search already had rate limits, which limited the number of searches that could be run [redacted], the scrapers appeared to be collecting data within these rate limits by using an extensive set of bots [redacted], with each bot operating at or below the applicable rate limit. MPIL stated that given the limited user usage of the functionality in practice, the ability to search for users by phone number or email address on Facebook Search was removed as a failsafe way to eliminate this functionality as a contact scraping vector. This mitigation was implemented in late March 2018.

[67] Appendix D.7c at 2-3. Appendix D.12e amended this submission to remove reference to Messenger CI at 3.

[68] See Appendix D.1b page 2 and Appendix D.3b at 6-7.

109. Soon after turning off the ability to search by phone number or email address on Facebook Search, an anomalous increase in usage of the Facebook account recovery feature was observed. The Account Recovery feature enables a user to initiate an account recovery flow by typing in the phone number or email address associated with their account. At the time, this would then display certain basic profile information corresponding to the account the user was seeking to recover and initiate a user flow to verify that the user was the authorised user of the account. It was determined that this surface was being used to scrape the basic profile information that was displayed. In response, the feature was modified so as to avoid returning any identifying profile information in response to an input phone number or email address in scenarios where the user is not using a device associated with the account sought to be recovered (or where other trust signals were lacking). These changes to Facebook Search and Account Recovery were announced in a blog post on 4 April 2018, explaining that the features had been abused to scrape public profile information.

110. MPIL stated that

> *ordinary, manually set rate limits are the only standard measure commonly employed by companies to address scraping.* [69]

111. The Preliminary Draft Decision initially stated, on the basis of MPIL's August 2021 and April 2022 submissions that in order to address the scraping issue, MPIL reduced the rate limits on Messenger Contact Importer [redacted] [70]

[69] Appendix D.7c at 3

[70] See Appendix D.10c at 1-2 and Appendix D.4c pages 1-2, 14 and 17: *"Specifically, pre-2018, and continuing until the discovery of phone number enumeration scraping on Facebook Search in March 2018: ● [redacted] there was a limit [redacted] If this limit was surpassed, the user would have to solve a captcha in order to conduct any further searches—specifically, [redacted]. ● [redacted], there was a rate limit [redacted]*
After the discovery of phone number enumeration on Facebook Search in March 2018, as an immediate mitigation measure, [redacted]
"As explained in the Response to Query 1 above, prior to the Relevant Period, Facebook Search was subject to rate limits of [redacted] [redacted] [redacted] [redacted]. Facebook CI was subject to a rate limit of [redacted] Messenger CI was subject to rate limits [redacted]"
"The March 2018 integrity review was an ad hoc review undertaken by the Facebook Search team to look for patterns of search queries on the feature indicative of scraping. Among other log data examined as part of the review, [redacted] This discovery led to the mitigating measures implemented in April 2018, as discussed in Response to Queries 3-5 in the May 2021 Response."
"The rate limit applicable to Facebook CI was changed in April 2018 from [redacted]

112. However, per its submissions of 14 July 2022 and, its amended submissions of 11 August 2022, MPIL updated this submission to state that [redacted][71]

113. The rate limits on Facebook Contact Importer at the commencement of the Temporal Scope was similarly set at [redacted]. However, there was no corresponding further reduction on the rate limits made in September 2018. MPIL stated that

> *…this remained the applicable rate limit for Facebook CI and Friend Centre[72] throughout the temporal scope…[73]*

114. In this respect, MPIL similarly stated on 27 April 2022:

> *As at the commencement of the temporal scope,* [redacted] […] [74]

115. With regard to Messenger Search for Mobile Devices, MPIL stated:

> *As at the commencement of the temporal scope, the rate limits for Messenger Search on the Messenger mobile app were:* [redacted] *These same rate limits applied to Messenger Contact Creator which relied on the same underlying phone number lookup functionality.*

[71] Appendix D.12g at 2.

[72] Appendix D.8d page 9: *"Facebook Friend Centre – a contact importation surface, which otherwise had the same 'look and feel' as Facebook CI, to which users could navigate any time after registration in order to upload contacts to find 'Friends'."*

[73] Appendix D.10c page 1. It should be noted that per Appendix D.4c page 17, the rate limit for Facebook CI was changed in April 2018 [redacted]

[74] Appendix D.10c at 1.

On 12 September 2018, the rate limits for searches by phone number were amended to [redacted]

[redacted] *[75]*

116. MPIL stated that:

> *In spite of these efforts, in August 2019 Facebook identified that scrapers were using bots for phone number enumeration to scrape public information via Messenger Contact Importer. Through this activity, the scrapers were able to access a large number of user profiles and obtain publicly shared information about those users while staying beneath Messenger's rate limits.*
>
> *To mitigate this risk, Facebook made changes to Messenger Contact Importer so that it no longer returned profiles that matched specific user phone numbers uploaded from a phone book. Similar changes were made to Instagram Contact Importer by September 2019."*[76]

117. In its amended submissions of 13 May 2021, provided on 11 August 2022, MPIL stated:

> *August 2019: Discovery of scraping abuse on Messenger Search ~~and Messenger CI~~*

[75] Appendix D.10c at 2. The underlined excerpts were added following the amendments of 11 August 2022 per Appendix D.12g at 2.

[76] Appendix D.1b at 3

> *In 2019, the External Data Misuse Team ("EDM Team") established a "red team", focused on identifying methods of scraping data on Facebook products and features so as to help the EDM Team improve anti-scraping controls. In late July 2019, the EDM Team reported that it had found feasible methods of conducting phone number enumeration scraping on the Messenger mobile app's search feature ("Messenger Search") ~~and Messenger CI~~. The methods involved using large numbers of bots to emulate users using ~~these~~ this feature~~s~~ on the Messenger mobile app. While the total usage by each bot would stay within applicable rate limits, the lookups could nonetheless potentially be run at scale through the parallel use of the numerous bots. Informed by these findings, the EDM Team discovered patterns of Messenger usage consistent with the scraping method identified by the red team, indicating that scraping was likely occurring via ~~these features on~~ Messenger Search.*
>
> *This discovery led to the following changes being made to Messenger Search, Messenger Contact Creator and Messenger CI:*
>
> > *● Eliminating (i) the search-by-phone number functionality on Messenger Search on the Messenger mobile app in August 2019 and on Messenger Contact Creator in September 2019 and (ii) the search-by-email functionality on Messenger Search on the Messenger mobile app in September 2019; and*
> > *● While no evidence of scraping on Messenger CI was detected at this time, as a proactive measure, the ability to search for users by phone was eliminated from Messenger CI as well in September 2019. Similar to what had been done with Facebook CI previously, Messenger CI was modified so as to return friend suggestions only. ~~Temporarily disabling Messenger CI in September 2019. Messenger CI was relaunched in December 2019, having been modified so as to return PYMK suggestions rather than one-to-one matches, similar to the modification made to Facebook CI in December 2018 explained above.[77]~~*

118. In its amended submissions of 13 May 2021, provided on 11 August 2022, MPIL stated additionally in relation to Messenger Contact Creator:

> *September 2018: Discovery of scraping abuse of Messenger Contact Creator*
>
> *In September 2018, evidence of scraping on Messenger Contact Creator was discovered. Messenger Contact Creator was a variant of Messenger Search included on the Messenger mobile app: it was used to search for an individual user on the Messenger mobile app and, if that user was located on Messenger, to add that user to one's Messenger contacts. The activity detected on Messenger Contact Creator was determined to be phone number enumeration scraping in which the scrapers were registering large numbers of fake accounts to run phone*

[77] Appendix D.12d at 9-10. The underlining refers to the additions that MPIL made to the 13 May 2021 submission and the strike-through refers to the removals made.

> *number lookups through Messenger Contact Creator while staying within rate limits.*
>
> *There were advanced systems in place at the time to detect suspected fake accounts and to block them unless the user passed an authenticity check (such as a* [redacted]
>
> [redacted][78]

119. MPIL stated that Facebook Contact Importer was modified in October 2018, so that, instead of returning a list of Facebook users matched to uploaded contacts, the feature would return 'People You May Know'.

> *Facebook CI was modified on 10 October 2018 to stop Facebook CI from returning one-to-one matches for imported contacts and instead returning PYMK suggestions only. Friend Centre was similarly modified on 11 December 2018. Messenger CI was similarly modified on 6 September 2019.*[79] [80]

And per the May 2021 submissions:

[78] Appendix D.12d at 8.

[79] Appendix D.10c at 5

[80] Appendix D.10c at 5: *"MPIL wishes to correct the statement at page 10 of the May Response that Messenger CI was "temporarily disabled" in September 2019 and subsequently relaunched in a form that provided only PYMK suggestions. In fact, Messenger CI was modified in September 2019, so that it stopped returning one-to-one contact matches and instead returned only PYMK suggestions, starting at that time."*

> *In October 2018, the Abusive Account Detection Team discovered evidence of a large number of scripted accounts using Facebook CI for scraping activity - despite the mitigations made to Facebook CI in April and May 2018 described above. In particular, the team determined that scrapers had adapted their tactics to* [redacted]
>
> […]
>
> *In response to the discovery of these new tactics, further modifications were made to Facebook CI. Facebook CI had been designed to return Facebook users matched one-to-one with uploaded contacts, so that users could clearly see which of their uploaded contacts matched to users on Facebook. In* [October] *2018, however, Facebook CI was modified so that, instead of returning a list of Facebook users matched to uploaded contacts, the feature would return People You May Know ("**PYMK**") suggestions, which are based in part on matched imported contacts but* [redacted].
>
> […]
>
> *After this change was made, scraping activity was detected on Friend Centre, another Facebook CI surface, to which users could navigate after account registration. In response, Friend Centre was similarly modified to return only PYMK suggestions in December 2018.*[81]

120. Therefore, as this modification was applied to Facebook Contact Importer only and not to Messenger Contact Importer, a scraping vector identified for Facebook Contact Importer remained open on Messenger Contact Importer until the end of the Temporal Scope, when it too was modified. Similar to what had been done with Facebook CI previously, Messenger CI was modified so as to return friend suggestions only.[82]

121. In its response of 11 August 2022, MPIL clarified the rate limits in relation to Messenger Contact Importer and Messenger Contact Creator:

> *Rate limits were in place for Messenger CI throughout the Temporal Scope, but they were not lowered during the Temporal Scope in response to a known scraping incident involving the Messenger CI vector. As clarified in the Response, and explained in further detail in this letter, no scraping incident involving Messenger CI was detected during the Temporal Scope.*
>
> *In relation to rate limits for Messenger CI:*

[81] Appendix D.3b at 9. This excerpt originally referred to December 2018 but was amended and to insert the final paragraph, in Appendix D.12c at 9.

[82] Appendix D.12c at 10.

> - *Prior to the Temporal Scope, in response to scraping detected on Facebook Search in March 2018, the rate limits for Messenger CI were proactively tightened* [redacted] *per day to* [redacted]
> - *This rate limit of* [redacted] *uploaded contacts per day remained in place for Messenger CI throughout the Temporal Scope.*
>
> *For completeness, in relation to the rate limits for Messenger Contact Creator:*
>
> - *After scraping was detected on Messenger Contact Creator in September 2018, rate limits were tightened on the phone lookup functionality used by both Messenger Contact Creator and the standard Messenger Search feature, to* [redacted]*.*
> - *Further, separate rate limits were created limiting the addition of contacts through Messenger Contact Creator to* [redacted]

122. MPIL stated that:

> *The EDM Team supplanted the Anti-Scraping Team in 2019. The* [redacted] *currently employed by the EDM Team is attached hereto as Exhibit 3.*[83] [84]

123. The [redacted] provided by MPIL to the DPC included the following:

> [redacted]
>
> [redacted]

[83] Appendix D.4f.

[84] Appendix D.4c at 12.

[redacted][85]

[…]

[redacted][86]

124. MPIL stated that:

> *…the red team was established in the months following the creation of the EDM Team in May 2019 and was operational by July 2019. There was no determination that the red team was "required." The EDM Team simply chose to establish a red team focused on scraping as one component of the EDM Team's overall anti-scraping strategy. The use of a red team is a well-recognised method for proactively searching out potential attack vectors.*
>
> *As described in the May 2021 Response, in late July 2019 the red team reported that it had identified feasible methods of conducting phone number enumeration scraping on Messenger* [Search], *which led the EDM Team to discover patterns of Messenger* [Search] *usage consistent with those methods in August 2019.*[87]

125. And further that:

> *In 2019, the External Data Misuse Team ("EDM Team") established a "red team", focused on identifying methods of scraping data on Facebook products and features so as to help the EDM Team improve anti-scraping controls. In late July 2019, the EDM Team reported that it had found feasible methods of conducting phone number enumeration scraping on the Messenger mobile app's search feature ("Messenger Search") and Messenger CI. The methods involved using large numbers of bots to emulate users using these features on the Messenger mobile app. While the total usage by each bot would stay within applicable rate limits, the lookups could nonetheless potentially be run at scale through the parallel use of the numerous bots. Informed by these findings, the EDM Team discovered patterns of Messenger usage consistent with the scraping method*

[85] Appendix D.4e at 6.

[86] Appendix D.4e at 12.

[87] Appendix D.4c at 23. These submissions referred originally to Messenger CI but were amended to refer to Messenger Search in Appendix D.12d.

identified by the red team, indicating that scraping was likely occurring via these features on Messenger.

This discovery led to the following changes being made to Messenger Search and Messenger CI:

- *Eliminating (i) the search-by-phone number functionality on Messenger Search on the Messenger mobile app in August 2019 and (ii) the search-by-email functionality on Messenger Search on the Messenger mobile app in September 2019; and*
- [redacted] *Messenger CI was* [redacted] *modified so as to return* [redacted] *suggestions* [redacted] *similar to the modification made to Facebook CI* [redacted].[88]

126. MPIL indicated that it had bot detection measures in place throughout the Temporal Scope. MPIL's submissions dated 21 January 2022 provided:

> *To the extent there were (and are) measures widely used within the industry to reduce scraping risks, they are rate limiting and bot detection – both of which were in place throughout the temporal scope* [89]

127. MPIL provided the following details in relation to the bot detection measures deployed:

- *Systems designed to classify whether an account was fake.*
- *New policies for rule-based heuristics were developed regularly.*
- *Machine-based learning systems regularly trained with updated data.*
- *Where accounts were classified as not authentic, relevant systems would generally block the accounts from engaging in further activity.*
- *Policies in place to run at registration time in order to detect inauthentic accounts, including detection of accounts registered through an IP address registering large numbers of accounts within a short time frame.*
- *Post-registration classifiers employed that utilising several core methodologies for identifying inauthentic accounts, including identification of clusters of accounts, identification of accounts containing abusive content and 'deep entity classification' a system designed to catch inauthentic accounts that evade detection by other classifiers.*[90]

128. MPIL stated that:

> *...while the bot detection measures in place during the temporal scope were state-of-the-art, that does not imply that they were, or should be expected to have been, completely effective...*[91]

[88] Appendix D.3b at 9-10.

[89] Appendix D.8d at 2-3.

[90] Appendix D.10c at 2-5.

[91] Appendix D.10c at 5.

129. In the submissions of 27 April 2022, MPIL stated that:

> *there were sophisticated measures in place throughout the temporal scope to identify and block the creation of fake accounts, including "bots." These measures served to combat not only scraping but a wide range of abusive conduct that is facilitated through fake accounts.*

MPIL added that:

> *MPIL's processor, MPI, has published a formal paper that explains key aspects of its bot detection measures, including cutting edge machine-learning systems that examine many different properties and behaviours of user accounts.*[92] [93]

130. It is noted that the document provided as an exhibit in the submissions of 27 April 2022 makes no reference to scraping.

131. In its submissions of 21 January 2022, MPIL stated that:

> *The technical and organisational measures taken with respect to scraping during the temporal scope were appropriate and state of the art.*[94]

However, MPIL has failed to provide any further documentation to show its analysis of state of the art.

132. MPIL has also set out how subsequent to the Temporal Scope, it has implemented a number of changes and additional measures. These include:

> *Examples of some of the more significant initiatives of the EDM Team, taken from the second half of 2020 alone, include the following:*
>
> > *● The EDM Team completed the rollout of an initiative known as "Rate Limits Everywhere," which involved ensuring effective application of rate limits across all Facebook endpoints.*
> > *● The EDM developed a sophisticated system called Reputation Based Rate Limits ("RBRL"), which builds on Facebook's existing rate limit infrastructure. Whereas traditional rate limits are static, RBRL applies different rate limits to different users. Specifically, RBRL groups users into different tiers based on a "reputation" classification—which reflect the degree of confidence that the account is authentic based on the historical account usage—and applies more stringent limits to accounts in lower reputational tiers.*
> > *● The EDM Team also developed a system known as "Data Limits Everywhere," which goes beyond looking at the number of requests made on a particular endpoint by a particular user—which is the focus of traditional rate limits—and instead looks at the volume and nature of the data being queried in those requests. This system continues to be rolled out to an expanding number of endpoints.*

[92] Appendix D.10c at 2.

[93] Appendix D.10d Deep Entity Classification: Abusive Account Detection for Online Social Networks.

[94] Appendix D.8d at 2.

● The EDM Team built and rolled out a tool called "ScrapeScore," which assigns an endpoint a risk-weighted measurement of the data returned per request to a particular endpoint. The measurement is reflective of both the nature and the volume of the data returned. ScrapeScore helps the EDM Team prioritise its detection, prevention, and investigation efforts.
● The EDM Team identified numerous new behavioural signals to recognise potential scraping on Facebook's products, and also significantly improved its capabilities for collecting, storing, and classifying scraping signals.
● The EDM Team built more than ten new machine learning models designed to provide further protection beyond rate limits and existing integrity systems for endpoints that are sensitive and frequently targeted by scrapers.
● The EDM Team doubled the size of its Enforcement Team, completed several hundred investigations of individuals or entities suspected of engaging in scraping, and pursued over 150 enforcement actions.[95]

133. For the sake of completion, MPIL has also set out how it informed users:

● On 6 April 2021, details concerning the Dataset, including that the data was believed to have been scraped prior to September 2019 and that the scraping methods used to assemble the data were no longer possible, were published via Facebook Newsroom. This post also provided information to users about managing their privacy settings. https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/ (Exhibit 1);
● On 7 April 2021, a further article providing information to users regarding the Dataset was published here: https://www.facebook.com/help /463983701520800 (Exhibit 2);
● Users were also provided with a contact form (screenshot provided at Exhibit 3) so that they could raise questions or concerns on this matter to FIL directly. The contact form was launched on 9 April 2021;
● On 15 April 2021, further information about the efforts to combat scraping was published here: https://about.fb.com/news/2021/04/how-we combat-scraping (Exhibit 4); and
● On 19 May 2021, another article providing more details about our efforts to fight unauthorised scraping and "phone number enumeration" was published here: https://about.fb.com/news/2021/05/scraping-by-the-numbers/. (Exhibit 5).[96]

134. For the purposes of this Inquiry, I note MPIL's contention that its processing prior to these changes was compliant with the GDPR. The subsequent changes do not fall within the scope of this Inquiry, and I assume that these changes are without prejudice to

[95] Appendix D.4c at 5-6.
[96] Appendix D.7c at 3-4.

MPIL's prior contention that it has at all material times complied with the GDPR, including prior to the recent changes and during the periods considered by this Inquiry.

I. FINDING REGARDING ARTICLE 25(1) GDPR

135. As set out above, Article 25(1) states:

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

136. The obligation in Article 25(1) is scalable depending on the particular circumstances of the processing undertaken and the risks presented, as well as the state of the art and the cost of implementation. Therefore, I must have regard to these issues, as set out above, in determining whether the MPIL infringed Article 25(1) during the Temporal Scope.

137. In relation to scraping, MPIL has made a number of submissions that are relevant under Article 25(1). In its 13 May 2021 submissions, MPIL stated:

> *The Scraped Data Set was not collected through a "vulnerability", in the sense of any software bug or other unintended operation of Messenger CI. It was obtained through scraping, which is the automated collection of data from a website or app - data that is intended to be available to users, via manual means. The fact that a feature is scraped does not imply a defect with the feature itself.* ***To the contrary, the features believed to have been scraped in compiling the Scraped Data Set were useful features with benefits for ordinary users. They were intended to enable users to find other users by their phone numbers. The scraping was problematic only because it involved the automated use of these features by inauthentic accounts.***
>
> *With respect to scraping conducted through Messenger CI in particular, FIL believes that scrapers used bots to emulate people using Messenger CI to upload contacts. In this way, over time, the scrapers accumulated data on large numbers of returned contacts.* ***There was no "malfunctioning" of Messenger CI involved in this activity. The privacy settings related to the feature worked as designed; the feature would have returned data on matched users only to the extent permitted by those users' privacy settings. Likewise, the rate limits on the Messenger CI feature also functioned as designed. It is believed that the scrapers used numerous bots, each scraping within those limits, to collect information on a large number of users. This is a common fact pattern in scraping incidents and***

> ***is what makes scraping so difficult to limit; the user actions involved in scraping may be indistinguishable, from a technical standpoint, from those involved in normal use of a product.*** *Moreover, scrapers are constantly improving their tactics so as to more effectively blend in with ordinary traffic and evade detection. As the DPC is aware, this is an ongoing, industry-wide challenge affecting many companies with public-facing websites or apps.*[97] [emphasis added]

138. In its submissions of 21 October 2021, MPIL stated:

> [MPIL] *notes that there are no well-developed "industry standards" for anti-scraping controls, as there are for traditional security or privacy programs. Indeed, until recently, scraping has been largely regarded within the industry as solely an intellectual property issue (based on a concern about copying of site content). As far as* [MPIL] *is aware, ordinary, manually set rate limits are the only standard measure commonly employed by companies to address scraping. There is no industry consensus on whether other measures are necessary or appropriate. Nevertheless,* [MPIL] *and its processor,* [Facebook Inc, now Meta Inc], *consistently work against scraping to address scraping vectors where they are discovered and take action against perpetrators where possible.*[98]

139. In its submissions of 21 January 2022, MPIL stated:

> *The Relevant Features enable users to locate and connect with friends, family and communities around the world – as is central to Facebook's core purpose. The phone number-lookup functionalities that were part of the Relevant Features during the temporal scope were designed for this same core purpose, as they allowed users to locate others and to be located by others based on phone number, which is often the main contact point that one user may have for another. As is often the case with scraping, any efforts to limit the potential for scraping of these features came with a corresponding trade-off of limiting the potential usefulness of these important features for ordinary users.*[99]

Further:

> *The mere occurrence of scraping does not imply a failure of privacy by design. The fact that scraping occurred during the temporal scope does not of itself imply that Article 25(1) GDPR was infringed. The GDPR does not impose a strict liability standard. Article 25(1) GDPR requires the implementation of 'appropriate' measures that are 'designed' to implement data protection principles in an effective manner – not the elimination of all risk. Article 25(1) GDPR requires full consideration of (i) the benefits of the Relevant Features to users and their importance to the core purpose of Facebook; (ii) the privacy settings that enabled users to control who could search for them by phone number or who could view*

[97] Appendix D.3b at 3.

[98] Appendix D.7c at 3. See also Appendix D.8d at 2-3.

[99] Appendix D.8d at 2.

> *information in their profiles; and (iii) the lack of any state of the art that provided a means to prevent scraping of the Relevant Features altogether without eliminating beneficial functionalities useful to ordinary users.*[100]

140. Having particular regard to the risk of varying likelihood and severity for rights and freedoms of natural persons posed by MPIL's processing of personal data in the Relevant Features, I do not consider that the rate limiting and bot detection measures implemented by MPIL were sufficient for the purposes of Article 25(1) GDPR. As outlined above, the scope of MPIL's processing in the Relevant Features concerned a very large number of data subjects. This resulted in a particular risk of bad actors using the Relevant Features to acquire personal data due to the higher likelihood that random numbers and email addresses would match real Facebook users. There are a range of additional measures that MPIL could have implemented at the time to prevent such misuse of the Relevant Features during the Temporal Scope. While MPIL's non-implementation of any specific measure or group of measures does not in and of itself constitute an infringement of Article 25(1) GDPR, these measures provide context to the consideration of whether the measures implemented by MPIL were appropriate at the relevant time under consideration, and as to whether, taking into account the state of the art, the cost of implementation, the particular risks, MPIL, both at the time of the determination of the means for processing and at the time of the processing itself, implemented appropriate technical and organisational measures.

141. First, the contact matching features enabled scrapers to find exact matches for random phone numbers and email addresses. The purpose of these features was to enable Facebook users to find their friends and family. It is clear that MPIL could have implemented technical measures to mitigate the risk of scrapers finding such exact matches, while also enabling Facebook users to find other users for whom they already had their phone numbers or email addresses. This could have been achieved during the Temporal Scope by preventing exact matches in the results provided following lookups, and, instead, returning a selection of profile near matches that were not an exact match to the original phone number or email address inputted. Such a measure would have significantly mitigated the risk of scrapers directly linking Facebook users to phone numbers or email addresses, and was subsequently implemented by MPIL. It would have in effect severed the direct assignment of those numbers to individual accounts while maintaining the functionality of the feature for users who would have been able to identify the particular user they sought.

142. Second, rate limiting is an important measure to mitigate against the risk of misuse on the Relevant Features. By limiting the number of lookups, it is more difficult to carry out phone and email scraping. MPIL implemented further rate limits throughout the Temporal Scope, with the exception of for Messenger Contact Importer. It is clear that MPIL could have implemented lower limits during the Temporal Scope without impacting on genuine users' ability to connect with people known to them. Lower limits had been introduced with regard to Messenger Contact Creator, but similar mitigating measures were not put in place for Facebook Contact Importer nor Messenger Contact

[100] Appendix D.8d at 3.

Importer. It is unclear and unexplained why the Facebook Contact Importer rate was not limited during the Temporal Scope. Even in the circumstances, and given MPIL's submission in relation to the benefits of the Relevant Features quoted above, the reduced rate limit as set for Messenger Contact Creator was still set at such a high rate that it is difficult to understand why a lower rate could not have been set that would have had little impact on genuine users' use of the feature in a manner that maintained its functionality. It is unclear why, even where no scraping incident was detected involving Messenger Contact Importer during the Temporal Scope, given its susceptibility to scraping as with the other Relevant Features, no rate limits were introduced during the Temporal Scope at all.

143. Third, implementing 'captchas' and changing the presentation surface of the extracted data to avoid screen scraping automation are other areas which could have been considered in terms of mitigating risk. In particular, the addition of 'captchas', whereby typically distorted letters or numbers are required to be correctly entered or where images need to be evaluated, could have ensured that the use of the Relevant Features required the intervention of a human, creating an impediment which would have significantly hindered the mass-scraping activities while simultaneously ensuring that users remained able to avail of them and use them as intended.

144. Fourth, while MPIL established a "red team" to focus on identifying methods of scraping data on Facebook products and features in August 2019, implementing such a team earlier in the Temporal Scope would have been a relevant organisational measure to mitigate the risk as this team could have appropriately identified issues with the Relevant Features earlier, thus, enabling MPIL to implement measures appropriate to the dynamic nature of the risk. Given that the implementation of such a measure was open to MPIL, who state that they were aware of the use of scraping from early course, it is unclear why this was not done or considered.[101]

145. Implementing appropriate measures to ensure an appropriate response to potential incidents is crucial for implementing the data protection principles. As noted above, MPIL has submitted, but not explained, why the level of sampling of the scraped dataset undertaken by the EDM Team consisted of a subset of only 2,000 out of [redacted] discrete entries for which the UID had been confirmed to be valid. MPIL has not furnished any reasons as to why there appears to be so many UIDs in the dataset that do not correspond with valid Facebook IDs.

146. MPIL has not demonstrated that it has carried out any further analysis of other key database fields for the [redacted] records where there was not an exact hash match of the UID, e.g. MPIL has not excluded the possibility that other data fields in those entries (*first name, last name, phone number, city of residence*)[102] had been scraped from the Facebook platform while only the UID was corrupted by e.g. adding a leading space. In circumstances where the dataset was identified as the product of scraping from the

[101] At [10.33] of Appendix D.11c, MPIL note that the EDM team was created in May 2019. The reference to team here is to the "red team" per Appendix D.7c at 2-3.

[102] Appendix D.4c.

Facebook platform, it would appear reasonable to have obtained the raw, unhashed UIDs for the non-matching records to carry out further analysis.

147. Similarly, MPIL has failed to document any analysis carried out on the [redacted] records for which the hash of the UID did not match the hash of any valid Facebook UID. MPIL has not produced any analysis of whether the hash of the telephone number, email address or username has been compared to entries in the Facebook database.

148. These analyses are relevant measures for understanding the issues that led to the scraping and in understanding the extent of the data that was subject to the scraping. By carrying out such post-incident analyses MPIL could potentially identify further measures to mitigate the risk, both in terms of the data that already formed part of the scraped dataset, and in terms of mitigating the risk of further scraping in the future. The implementation of a diligent and thorough response to such incidents, particularly where there are risks involving a large amount of personal data and affects a large number of data subjects, among others, are central to the implementation of appropriate measures.

149. It is clear that there were a range of additional measures that MPIL could have implemented to further mitigate the risks posed by bad actors misusing the Relevant Features to acquire the personal data of Facebook users. However, Article 25(1) is not prescriptive as to measures that must be implemented; the state of the art of the range of potential measures that could be implemented, and which subsequently were implemented, are relevant. Therefore, MPIL's non-implementation of any specific measure or group of measures does not in and of itself constitute an infringement of Article 25(1) GDPR. Rather, in considering Article 25(1), I must consider whether the measures actually implemented were appropriate in the circumstances.

150. The EDPB has published Guidelines on Data Protection by Design and by Default, which summarise Article 25 as follows :

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

151. The requirement of effectiveness is a key element of Article 25(1), as set out in the EDPB guidelines :

> *Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.*

> *...First, it means that Article 25 does not require the implementation of any specific technical and organisational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk. Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing.*
>
> *...Second, controllers should be able to demonstrate that the principles have been maintained.*

152. MPIL's submissions provided:

> *It is important to appreciate that the mere fact that scraping occurred at all does not indicate that the measures in place to implement the data protection principles in accordance with Article 25(1) GDPR were not appropriate. Article 21(1) GDPR does not impose a strict liability standard. It requires only that 'appropriate' technical and organisational measures be implemented that are 'designed' to implement data protection principles in an effective manner.*[103]

153. I agree with MPIL's submission that Article 25(1) GDPR does not impose a strict liability standard. The requirement to implement the principles in an effective manner does not mean that any undesired outcome in respect of the data protection principles will necessarily be indicative of an underlying infringement of Article 25(1) GDPR. Rather, the central matter to be determined under Article 25(1) is whether the controller had implemented appropriate technical and organisational measures, which are designed to implement data protection principles in an effective manner, under the conditions set out in Article 25 GDPR, i.e. taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing.

154. While MPIL is not obligated to undertake any particular technical and organisational measures such as the ones set out above, the examples of measures provided above were all viable existing measures at the time of the Temporal Scope, some of which MPIL has indeed subsequently implemented, which would seem to show that the cost of implementation would not have posed an issue to MPIL. Indeed, MPIL has not itself in any of its numerous submissions identified any such issue related to the cost of implementation of these, or any other, measure.

155. In this regard, in its submissions of 14 July 2022, MPIL stated:

> *The PDD's apparent conclusion – that the rate limit and bot detection measures employed by MPIL were insufficient because they failed to prevent the scraping*

[103] Appendix D.8d at 3 and 11.

> *that occurred – is tantamount to applying a strict liability standard. This provisional finding also ignores the limitations of "state of the art" anti-scraping controls, and is therefore inconsistent with Article 25(1) GDPR's language requiring that appropriate measures be assessed "[t]aking into account the state of the art".* [104]

156. This attribution of "*the PDD's apparent conclusion*" that detection measures "*were insufficient because they failed to prevent the scraping that occurred"* did not appear in the Preliminary Draft Decision at all. Indeed, the paragraph of the Preliminary Draft Decision that MPIL references actually stated that "*Having particular regard to the risk of varying likelihood and severity for rights and freedoms of natural persons posed by MPIL's processing of personal data in the Relevant Features, I do not consider that the rate limiting and bot detection measures implemented by MPIL* ***were sufficient*** *for the purposes of Article 25(1) GDPR."*[105] I do not accept that this is tantamount to the application of a strict liability standard.

157. In its submissions of 14 July 2022, MPIL made a number of submissions:

> *The PDD does not include any analysis of, or identify, the "state of the art" regarding anti-scraping controls, nor does it cite any industry guidance or evidence of industry practice during the Temporal Scope that demonstrates that MPIL failed to implement "state of the art" measures. The PDD also does not rebut MPIL's submissions in the Inquiry that the measures implemented were in line with the "state of the art". As explained in the Issues Paper Response (which the PDD does not appear to dispute), the measures generally used by online platforms to reduce scraping risks – that is, the measures comprising the "state of the art" – consist of rate limits and bot detection.*[106]
>
> *Moreover, it should be emphasised that throughout the Temporal Scope there was no substantive guidance from the DPC or the EDPB on the application of Article 25(1) GDPR to scraping – indeed, there was no guidance on the application of Article 25(1) GDPR generally. In the absence of any such guidance, controllers – including MPIL – were entitled to rely on what they reasonably understood to be the state-of-the-art practices in the industry as the appropriate standard.*[107]

158. The Preliminary Draft Decision provides numerous alternatives that existed and could have been implemented but were not. Accordingly, I do not accept this submission. The suggestion that infringements of Article 25(1) could only arise where guidance specifically related to scraping had been provided would also render the GDPR unenforceable.

159. Further, MPIL stated:

[104] Appendix D.11c at [10.14].
[105] Appendix D.11a at [112].
[106] Appendix D.11c at [10.12].
[107] Appendix D.11c at [10.15].

> *To the contrary, the effect of changing Facebook CI and Messenger CI to return only friend suggestions was to eliminate direct contact matching functionality and, thereby, one of the purposes of Contact Importer, i.e. the purpose of enabling users to easily identify which of their mobile phone contacts were Facebook or Messenger users and to connect with them specifically.* […]
>
> *It would have made no sense to return friend suggestions to the user in that context, any more than it would make sense for a phone carrier to suggest friends to a caller when they dial the number of a friend.* […]
>
> *Accordingly, there is no basis to conclude that MPIL was required under Article 25(1) GDPR to substitute friend suggestions for direct matching on any of the Relevant Features.* […]
>
> *Indeed, still today, other leading and popular services besides Facebook and Messenger, such as Skype, LINE, Viber, and others, offer the ability to look up users directly by their phone numbers. Others, such as Snapchat, LinkedIn, TikTok, and Clubhouse, likewise offer the ability for users to upload phone numbers of their contacts and view those contacts that directly match users of the service. These are useful functionalities that online services should have the right to offer to their users (and their users should have the right to use).*[108]

160. I do not accept the premise of what is being asserted here. While it may have been more convenient for there to be direct matches, no reason has been put forward as to why this was absolutely necessary, or why not doing so would have rendered the Relevant Features inoperable. This submission seems to suggest that users would be incapable, without the Relevant Features making direct matches, of recognising who their friends were. The conflation of searching for a friend on a social network with a direct phone call is not a tenable comparison.

161. Further, per MPIL:

> *By contrast, Facebook CI could be used to import a user's entire address book, which could contain hundreds or thousands of contacts. Imposing the restrictive rate limits that were imposed on Messenger Contact Creator in September 2018 – [redacted] – would have made no sense in the context of Facebook CI and would have crippled the functionality of the feature.* […]
>
> *Second, Facebook CI was fundamentally changed in any event in response to the October 2018 scraping incident so as to return only PYMK suggestions and to no longer return direct contact matches. As the PDD itself acknowledges at paragraph 113, this change effectively severed the link between the phone numbers of the imported contacts and the results returned by the feature, thereby eliminating this as a potential scraping vector altogether. Consequently, the*

[108] Appendix D.11c at [10.21]-[10.23].

> *mitigation rendered the rate limits on the feature moot: no matter how many times the feature was used or how many contacts were uploaded by a user, direct matches would not be returned, frustrating any attempt to link any uploaded phone numbers to specific users.*[109]

162. Further:

> [A]*s MPIL has previously explained in the Inquiry, captchas were used during the Temporal Scope as part of the bot detection systems.* […]
>
> *To the extent the DPC is suggesting that captchas should have been shown to every user before they could use the Relevant Features, such a measure would have had very significant disadvantages for users and would not have been a proportionate or appropriate way to address scraping risks. Captchas present digital literacy and accessibility challenges for a significant number of users. Digital literacy varies widely among users, and a portion of users are confused by captchas (which are intended to be somewhat tricky to solve). Additionally, some Facebook and Messenger users are vision impaired or have other disabilities that create accessibility barriers to solving captchas.* […]
>
> *That is part of the reason why captchas are instead used in a more targeted fashion by MPIL, as part of the bot detection systems, which show a captcha to a user only where there is some signal indicating that the user's account may be fake.* […]
>
> *A further problem with the idea of using captchas as a gating mechanism for features that could be used by fake accounts is that there would be no clear place to draw the line. Many features are potentially subject to various kinds of misuse. Features used for sending messages to other users can be used to send spam. Features used for creating posts or comments can be used to spread disinformation. Features used to send friend requests can be used for fraud. Yet if users were required to pass a captcha every time they wished to use these or any other features that could potentially be misused, much of their time on the services would be spent completing captchas, making the services unwieldy to use and undermining their fundamental purpose of enabling users to seamlessly connect with one another.* […]
>
> *Finally, it should be noted that captchas themselves are by no means a foolproof mechanism for preventing scraping or other abusive activity in any event. Services are available on the internet that offer to solve captchas for scrapers and other abusive actors, at rates as low as a dollar per 1,000 captchas solved.*[110]

163. In its response of 11 August 2022, in relation to captchas, MPIL stated:

[109] Appendix D.11c at [10.25]-[10.26].

[110] Appendix [10.27]-[10.31].

As explained in the Response (at paragraphs 10.12 and 10.27), and in MPIL's April 2022 Response (in response to Question 2), captchas were during the Temporal Scope, and continue to be today, a standard part of the bot detection systems that are used to detect inauthentic accounts. Where these systems flag an account as potentially inauthentic, the account is checkpointed so that it cannot be used unless and until the user of the account clears a captcha or a manually reviewed authentication challenge.

However, as explained in the Response (at paragraphs 10.28-10.32), captchas were not part of the "flow of the Relevant Features"; that is, a user did not have to pass a captcha simply in order to use the Relevant Features. As explained in the Response (at paragraphs 10.28-10.32), such a practice was (and is) not considered to be a proportionate measure to address scraping risks, as captchas impose digital literacy barriers to use and accessibility challenges for significant numbers of legitimate users, and moreover, there would be no clear place to draw the line if captchas were deployed wherever features are potentially subject to misuse by inauthentic accounts, as many features are potentially subject to such abuse, not merely the Relevant Features.

Accordingly, while captchas were (and are) deployed by bot detection systems where there is reason to believe an account may be inauthentic – including in the context of the Relevant Features – captchas were not a gating mechanism that users of the Relevant Features had to pass through as a matter of course (nor are they so used today).

[…]

MPIL is unaware of any contemporaneous documentation from the Temporal Scope in which MPIL "established what was the state of the art for scraping". As MPIL has explained in the Inquiry, there are, and were during the Temporal Scope, no recognised industry guidelines setting out any state of the art with respect to scraping. Further, online services do not generally publish or disclose specific details about how they combat scraping – in part because doing so would provide threat actors with actionable intelligence that they could use to evade anti-scraping measures. However, as explained in the Response, at a general level MPIL understood the state of the art with respect to scraping to consist of rate limits and bot detection measures. These types of measures are, and were during the Temporal Scope, generally understood in the industry as the sorts of measures appropriate to combat scraping.

MPIL is likewise unaware of documentation formally "taking into account" these measures as "the state of the art". However, these types of measures were clearly recognised as appropriate, as they were implemented on Facebook and Messenger during the Temporal Scope, including with respect to the Relevant Features, as discussed in MPIL's submissions. Further demonstrating MPIL's commitment to developing the state of the art in this area, the EDM Team was

> *launched during the Temporal Scope, and it has continued to invest substantial resources in refining Meta's anti-scraping measures in order to ensure that they are as sophisticated as possible. This is reflected, for example, in the various additional types of customised rate limits and other customised scraping-detection systems that have been developed and implemented by the EDM Team, as discussed in MPIL's August 2021 submission (in response to Query 5).*[111]

164. The use of captchas was one of numerous avenues that were open to MPIL. MPIL has not provided any evidence that would have posed an insurmountable hurdle to users. By no means have captchas been proposed as a panacea, rather a measure that could have been employed to mitigate against the risk of scraping, amongst other measures.

165. While MPIL submits here that captchas *were* used, MPIL's previous response from August 2021 notes that they were in use pre-2018 until March 2018; to detect and block fake accounts, particularly when a new account was registered; and as part of the rate limits for a particular endpoint.[112] This would seem to suggest that an account could exhibit sufficiently 'normal' activity to pass the initial checks and then run multiple CI/Search functionality before running into a rate limit, which is difficult to square with MPIL's opposition to captchas in the later submissions.

166. While it may be that captchas reduces the accessibility and ease of use, MPIL has provided no risk assessment or substantiation of its assertion that their use would have "*very significant disadvantages for users*", or for "*for a significant portion of users*." Indeed, in spite of this submission, MPIL continues to utilise captchas in a limited manner despite the claimed issues.

167. I consider that the technical and organisational measures implemented by MPIL during the Temporal Scope were not sufficient to appropriately implement the data protection principles as required by Article 25(1) GDPR and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects. I consider that MPIL failed to implement appropriate measures in respect of the purpose limitation principle provided for in Article 5(1)(b) GDPR. The lack of appropriate measures exposed the Relevant Features to use by bad actors to create a data set, rather than finding profiles of Facebook users known to them. The measures implemented were not appropriate to implement the principle that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. I also consider that MPIL failed to implement appropriate measures in respect of the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR. The lack of appropriate measures enabled bad actors to use the Relevant Features to discover whether random combinations of numbers and letters correspond to valid phone numbers and email addresses, and, if so, to discover the identity of the Facebook user who owns the relevant phone number or email address. The measures applied were not appropriate to implement the principle that personal data shall be processed in a manner that

[111] Appendix D.12b at 10-11.

[112] Appendix D.4c at 1, 6, 7, 13, 14 and 19.

ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.

168. The obligation rested on MPIL to choose measures that were designed to implement these data protection principles in an effective manner. While MPIL implemented rate limits and bot detection measures to mitigate the risk, I do not consider that these measures were sufficient at mitigating the risk of fake account activity and bots from acquiring data below the rate limits and, indeed, do not appear to have been effective. I have had regard to the risk associated with the processing, the potential cost of implementing additional measures to mitigate those risks, and the state of the art regarding the potential measures that MPIL could have implemented. In the circumstances, I consider that the technical and organisational measures implemented by MPIL were not appropriate.

169. I find that MPIL infringed Article 25(1) GDPR by failing to implement appropriate technical and organisational measures, which are designed to implement data protection principles, specifically the principles provided for in Article 5(1)(b) and (f) GDPR, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

J. FINDING REGARDING ARTICLE 25(2) GDPR

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

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

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

171. Two distinct issues arise in relation to the question of MPIL's compliance with data protection by default during the Temporal Scope. First, the searchability settings for users regarding the Relevant Features were automatically set to include each user's phone number and email address. Users were required to navigate to the Privacy section of the settings to remove this. MPIL outlined the available settings and submitted that the default searchability setting for phone numbers during the Temporal Scope was 'Everyone':

> *The available settings during the Relevant Period for searchability by phone number or email address on Facebook and Messenger were "Everyone", "Friends of Friends", "Friends", and, as of May 2019, "Only Me". There were two separate searchability settings available - one for phone number searches and one for email address searches. These were located in the "Privacy" section of the main settings menu in a user's account. Users could navigate to this menu directly from the*

> *Facebook homepage after logging in. The default setting for both phone number and email address was 'Everyone'.*[113]

172. MPIL stated:

> *A user's "searchability" settings are account-level settings that govern who can look up the user by a phone number (i.e. who can see the user account identity based upon entering a corresponding phone number).*
>
> *During the temporal scope, the available settings for searchability by phone number on Facebook and Messenger included 'Everyone', 'Friends of Friends', 'Friends' and, from May 2019 forward, "Only Me". If User A's phone number searchability setting was set to 'Everyone', this would mean that anyone could look up User A on Facebook using User A's phone number (and have User A's Basic Profile Information returned as a result). Alternatively, a user could restrict their searchability setting by choosing an option other than 'Everyone'. For example, if User A's phone number searchability setting was set to 'Friends', this would mean that only Friends of User A could look up User A on Facebook using User A's phone number (and have User A's Basic Profile Information returned as a result). Searchability settings were located in the 'Privacy' section of the main settings menu in a user's account. Users could navigate to this menu directly from the Facebook homepage after logging in. The default searchability setting for phone numbers during the temporal scope was 'Everyone' (as remains the case today). It is important to note that making the default searchability setting "Everyone" was not an arbitrary decision; it reflects a core value of Facebook: to connect people, around the world, with friends, family, and meaningful communities. When a new user—again, take Jane—joins Facebook, she has not yet established any connections with other Facebook users. That is, she has no 'Friends'. If, by default, only Friends of Jane could search for and find her on Facebook, then by definition no one could find Jane on Facebook (as she would have no Friends in the first place). In particular, anyone who had imported Jane's phone number or email address would not receive a recommendation suggesting Jane as a Friend on that basis. By the same token, if Jane's potential Friends had their searchability set to Friends only, then Jane—who, again, has no Friends yet—could not search for and find those potential Friends either. In particular, Jane would not receive recommendations based on the phone numbers or email addresses of those individuals if she were to upload them using contact importer functionality. Thus, setting. searchability to Friends by default (rather than Everyone) would significantly frustrate the purpose for which a user joins Facebook, as it would make it difficult for a new user to find Friends, or for potential Friends to find them, in the first place. Based on a review of sample data from the Scraped Data Set (as described in the Response 4 of the August Responses), as well as a review of the codebase underlying the Relevant Features, there is no reason to believe the Scraped Data Set contains any users who limited their phone number searchability setting, i.e., the setting that determines who can look up a user by phone number. Code reviews have confirmed that each of the Relevant Features would check a*

[113] Appendix D.3b at 16.

> *user's searchability settings before returning the user's information in response to a phone-based match. Only if the user's searchability setting allowed "Everyone" to look them up by phone number would the user's information be returned in response to a query by someone lacking any friend or friend-of-friend connection to the user. For this reason, Meta Ireland believes that the Scraped Data Set contains information only for users whose searchability settings allowed "Everyone" to search for them by phone number.*[114]

173. As set out in the Preliminary Draft Decision, the second issue arising was that it had appeared that where a user added their phone number for 2FA, the user flow for doing so automatically included the phone number as searchable in the Relevant Features and users were required to subsequently change their settings after providing their phone number to prevent it from being searchable. It had appeared that, during the Temporal Scope, where a user attempted to add their phone number to their account for the purpose of 2FA,[115] the provided flow did not allow users to solely provide their number for 2FA. Instead, the flows during this period also included the additional purposes of uploading the number to '*find friends, and more*' with no mechanism in the flow to exclude the additional purposes. This, combined with the default setting of '*everyone*' with regards to searchability, appeared to suggest that all users who uploaded their phone number for the purpose of 2FA were, by default, searchable by their phone number and subject to the reverse-lookup functionality.

174. However, in MPIL's submission of 14 July 2022, it stated that:

> *If a number was uploaded using a flow solely used for providing a phone number for 2FA purposes, a user could not be looked up based on that number, regardless of the settings otherwise applicable to their account, and regardless of the phone searchability setting set by the user for other numbers that may be linked to their account.*[116]

175. As noted in the Preliminary Draft Decision and MPIL's submissions of 14 July 2022, the subject flows indicated that the phone numbers added through the flows could be used to help users 'find friends', and so this was indeed capable of happening. Direct questions had been posed in this respect and on 25 March 2019, MPIL submitted:

> *There is a link to Facebook's Data Policy (signified by "find friends, and more"), which explains the purposes for which such data could be used by Facebook, as well as clarifying the additional processing that will be applicable to this telephone number since the user is choosing to use the 2FA feature ("you can reset your password if you ever need to"). When a user clicks 'and more' from the screen to add a contact data phone number to their Profile from within the set-up flow for 2FA, they are taken directly to Facebook's Data Policy, …*

176. Further queries in this regard were also posed by the DPC, which were answered by MPIL on 11 August 2022. MPIL stated:

[114] Appendix D.8d at [15]-[19]. See also Appendix D3.6 at 11-12.

[115] Appendix D.4j and Appendix D.5c.

[116] Appendix D.11c at [5.2]. See also [5.1]-[5.4] and [13.1]-[13.6].

To clarify:

- *In previously referring to "phone numbers provided solely for 2-FA purposes," MPIL was referring to phone numbers that were added to an account solely through a flow for providing a phone number that would be used to send the user two-factor authentication prompts ("2-FA Flow"), as opposed to also being added by the user to their account through different flows not specifically relating to 2-FA. Many users who sign up for 2-FA choose to use the same phone number already registered to their profile. In referring to "phone numbers provided solely for 2-FA purposes," therefore, MPIL was intending to distinguish that situation and to refer instead to phone numbers provided only through a 2-FA Flow. This is why MPIL specifically defined the term "2-FA Numbers" in its submissions to mean "phone numbers that a user added to an account solely through a flow used for providing a phone number for two-factor authentication.*

- *MPIL did not mean to suggest that these 2-FA Flows themselves specifically advised users that the only purpose for which MPIL could process 2-FA Numbers was to support two-factor authentication. As the DPC notes, and as MPIL has explained in the Response, the relevant flows informed users that the submitted phone numbers could be used for other purposes, including finding friends. Nonetheless, as a matter of internal policy, MPIL did not use 2-FA Numbers for purposes of returning contact matches in the Relevant Features during the Temporal Scope. For that reason, 2-FA Numbers were not subject to phone number enumeration scraping through the Relevant Features and, therefore, MPIL considers that 2-FA Numbers fall outside the scope of the Inquiry.*

  To ensure that MPIL's terminology in relation to this issue is clear and consistent, MPIL has inserted a footnote in its May 2021 submission to clarify the intended meaning of the phrase "phone numbers provided solely for 2-FA purposes."

  MPIL also takes this occasion to note that, in previously stating that 2-FA Numbers were not used for purposes of the Relevant Features or to help users find friends, the submissions were intended to refer specifically to 2-FA Numbers not being used to return contact matches in the Relevant Features – as that is the issue relevant to whether 2-FA Numbers were subject to phone number enumeration scraping through the Relevant Features. For the sake of completeness, however, MPIL wishes to add that some 2-FA Numbers were used to generate PYMK/friend suggestions during the Temporal Scope. Specifically, in parallel to responding to your letter, MPIL has learned that there was a separate internal system used to prevent 2-FA Numbers from being used to generate PYMK/friend suggestions during the Temporal Scope, different from the internal system used to prevent them from being used to return contact matches. Some 2-FA numbers were not covered by this separate

> *system, which would therefore have allowed some 2-FA Numbers to be used to generate PYMK/friend suggestions during the Temporal Scope.*
>
> *MPIL apologises for not learning of this and therefore clarifying sooner in the Inquiry. However, this issue does not impact whether 2-FA Numbers were susceptible to scraping. As recognised by the DPC in the PDD (at paragraph 113), PYMK/friend suggestions were not subject to phone number enumeration scraping, since any link between the suggestions provided to a user and the phone numbers uploaded by the user was obfuscated. This correction thus does not change MPIL's position in the Inquiry with respect to 2FA Numbers; it is noted here, and where relevant in the redlines of the various submissions, to clarify this point in the interest of full disclosure.*[117]

177. In its amended submissions provided on 11 August 2022, MPIL amended references in previous submissions to in relation to the above.[118]

178. In circumstances where it has been clarified by MPIL that telephone numbers provided through the 2FA entry flow were not used for individual matching of searched telephone numbers, I accept that this issue is not relevant to my consideration of Article 25(2) within the scope of this Inquiry. Therefore, in the context of MPIL's compliance with Article 25(2), this Decision considers the first issue only, of the searchability settings for users regarding the Relevant Features being automatically set to include each user's phone number and email address is relevant to the scope of this Inquiry.

179. MPIL outlined that the purpose of the searchability settings were designed to enable people to find their friends by entering their phone numbers or email addresses. MPIL also outlined that this feature is especially useful in countries where large numbers of people share the same or similar names. MPIL further outlined that it is a core value of Facebook to connect people, around the world, with friends, family, and meaningful communities and that providing users with that experience often depends on their searchability settings under the Relevant Features.

180. In its submissions dated 13 May 2021, MPIL stated that

> *The privacy settings related to the feature worked as designed; the feature would have returned data on matched users only to the extent permitted by those users' privacy settings. Likewise, the rate limits on the Messenger CI feature also functioned as designed. It is believed that the scrapers used numerous bots, each scraping within those limits, to collect information on a large number of users.*[119]
>
> […]

[117] Appendix D.12b.

[118] See, for example, Appendix D.12d at 12.

[119] Appendix D.3b at 3.

> *It is important to note that making the default searchability setting "Everyone" was not an arbitrary decision; it reflects a core value of Facebook: to connect people, around the world, with friends, family, and meaningful communities. Providing new users with that experience - a core purpose of joining Facebook - often depends on both their and other users' searchability settings being set to Everyone.* […]
>
> *Thus, setting searchability to Friends by default (rather than Everyone) would significantly frustrate the purpose for which a user joins Facebook in the first place, as it would make it difficult for a new user to find Friends, or for potential Friends to find them, in the first place.*[120]

181. Users upload their phone numbers and email addresses to Facebook for a variety of purposes, including as a unique identifier, and, indeed, for searchability. However, the Relevant Features enabled the use and input of random combinations of numbers in order to identity particular accounts. Where this happened, this has the effect of confirming a particular sequence of numbers as a phone number and as belonging to a particular user, allowing the obtaining of the personal data of that user. MPIL asserts that phone numbers were not collected from user profiles but rather they were instead supplied by the scrapers as part of their scraping method. This is misconceived. While the scrapers inputted the number sequences, it was the Relevant Features that matched them to a user account and thus confirmed them as a phone number. The utilisation of the Relevant Features is distinct in terms from opting into the searchability setting. In the absence of the Relevant Features, they would have remained number sequences and it was the Relevant Features that confirmed that they were indeed phone numbers.

182. By setting the searchability settings for users regarding the Relevant Features automatically to include each user's phone number and email address, MPIL made that personal data accessible without the individual's intervention to an indefinite number of natural persons. This exposed the personal data to scrapers, who could potentially access it using reverse-lookup functionality. As a result, the numbers and email addresses were made accessible without the data subjects' intervention to an indefinite number of natural persons. Also as a result, the Facebook profiles were made searchable to legitimate users via the Relevant Features, even where the data subject did not submit their phone number for searchability purposes. MPIL failed to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. By automatically processing such phone numbers and email addresses in the Relevant Features, and in light of how users upload their phone numbers and email addresses to Facebook for a variety of purposes, MPIL failed to implement appropriate measures to ensure that by default, only personal data which are necessary for each specific purpose of the processing were processed. Accordingly, I find that MPIL infringed Article 25(2) GDPR through failing to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed. In addition, MPIL

[120] Appendix D.3b at 16.

infringed Article 25(2) because the default settings used by MPIL failed to ensure that by default the personal data were not made accessible without the data subjects' *intervention to an indefinite number of natural persons*.

K. CORRECTIVE POWERS

183. I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my finding that MPIL has infringed Article 25(1) and 25(2) GDPR.

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

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

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

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

    (1) An order pursuant to Article 58(2)(d) to MPIL to bring its processing into compliance with the GDPR in the manner specified below;

    (2) A Reprimand to MPIL pursuant to Article 58(2)(b) GDPR; and

    (3) Two administrative fines in the amount of €150 million, and €115 million respectively.

187. I set out further detail below in respect of each of these corrective powers that I have decided to exercise and the reasons why I have decided to exercise them. This document is my Final Decision. Following the Preliminary Draft Decision, MPIL made specific submissions on 14 July 2022 in relation to the individual corrective powers, which I have taken into consideration.

L. ORDER TO BRING PROCESSING INTO COMPLIANCE

188. Article 58(2)(d) GDPR provides that a supervisory authority shall have the power

> *to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period*

189. Having considered that the measures implemented by MPIL to address the scraping issue, I do not make an order under Article 58(2)(d) in relation to Article 25(1) GDPR.

190. However, with regard to Article 25(2), I consider it appropriate to order MPIL to bring the relevant processing into compliance with Article 25(2) GDPR.

191. Specifically, to the extent that MPIL is engaged in ongoing processing of personal data which includes a default searchability setting of 'Everyone', this order requires:

(1) MPIL to implement appropriate technical and organisational measures regarding the Relevant Features in respect of any ongoing processing of personal data, for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, and that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. This order is made to ensure compliance with Article 25(2) GDPR.

192. I consider that this order is necessary to ensure that full effect is given to MPIL's obligations in relation to the data protection by default infringement outlined above. The substance of this order is the only way in which the defects pointed out in this Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that I am of the view that this power should be imposed. I note too that MPIL asserts that it has expanded its mitigation efforts since the Temporal Scope.[121] This Decision does not make findings regarding the appropriateness of the measures implemented in respect of MPIL's ongoing processing with regard to the Relevant Features beyond the Temporal Scope, although they have been mentioned for completeness. In any event, MPIL is accountable for ensuring that its ongoing processing with regard to the Relevant Features is compliant with the GDPR. In this regard, the DPC reserves its right to commence further statutory inquiries, if necessary.

193. Having regard to the non-compliance in this Decision, in my view, such an order is proportionate and is the minimum order required in order to guarantee that compliance will take place in the future. I am satisfied that the order is a necessary and proportionate action.

194. I therefore require MPIL to comply with the above order within three months of the date of notification of any final decision. Further to this, I require MPIL to submit a report to the DPC within that period detailing the actions it has taken to comply with the order.

M. REPRIMAND

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

[121] Appendix D.8d at [4] and [36]-[39].

196. The Preliminary Draft Decision proposed to impose such a reprimand. In its submissions of 14 July 2022 in response, MPIL made a specific submission with regard to the imposition of a reprimand based on Recital 148 GDPR.[122] MPIL asserted that Recital 148 must be interpreted to mean that a supervisory authority has the corrective power to impose either a reprimand or a fine, or that where there is a minor infringement a reprimand without the imposition of an administrative fine "*should be the maximum extent of any exercise of corrective powers*."[123] The thrust of this submission, is that the reprimand power can only be used as an alternative to administrative fines for minor infringements.

197. Such an interpretation is plainly misconceived and entirely artificial - one which would ignore the actual wording of both Article 58 and Recital 148 GDPR. As set out above, Article 58(2) GDPR states that each supervisory authority has the corrective power, *inter alia*:

> *(i) to impose an administrative fine pursuant to Article 83,* ***in addition to****, or instead of* ***measures referred to in this paragraph****, depending on the circumstances of each individual case*
>
> [emphasis added]

198. Indeed, Recital 148 GDPR states in full:

> *In order to strengthen the enforcement of the rules of this Regulation, penalties* ***including administrative fines*** *should be imposed for any infringement of this Regulation,* ***in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation****. In a case of a <u>minor infringement</u> or if the fine likely to be imposed would constitute a <u>disproportionate burden to a natural person</u>, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.* [emphasis added]

199. Article 58(2)(i) GDPR is clear, as the text of the provision states on its face that a supervisory authority has the power to impose an administrative fine "**in addition to…measures referred to in this paragraph**", where the second measure in that paragraph is to issue a reprimand. The other measures include warnings, orders to bring into compliance, orders to communicate a personal data breach to a data subject,

[122] Appendix D.11c at [10] on 5, and at [38]-[40] on 62.
[123] Appendix D.11c at [11] on 62.

temporary or definitive limitations including a ban on processing, orders for rectification/erasure/restriction of processing and notification of such an order, withdrawal of certification and suspension of data flows.

200. Recital 148 GDPR is clear that administrative fines "**should be imposed for any infringement**" of the GDPR "**in addition to or instead of appropriate measures**". That Recital advises that a supervisory authority ***may*** issue a reprimand instead of a fine for a minor infringement or if the burden of a fine on a natural person would be disproportionate. The Recital does ***not*** advise that the corrective measures in Article 58(2) are mutually exclusive, such that a supervisory authority should not impose both a reprimand and an administrative fine – even where there is (only) a minor infringement. Rather, Recital 148 GDPR envisages the discretionary imposition of a reprimand instead of an administrative fine where there is a minor infringement, or if the fine likely to be imposed would constitute a disproportionate burden to a natural person. It does not in any way vitiate the use of a reprimand where an administrative fine is to be imposed.

201. Even in the premises of MPIL's submission – that where there is a minor infringement, a reprimand "*should*" be issued instead of an administrative fine –MPIL's interpretation ignores the actual words of Recital 148 which states "*a reprimand **may be** issued instead of a fine*" [emphasis added]. In any event, as set out above, I do not accept that MPIL's infringement is minor.

202. I have decided to impose a reprimand on MPIL for the infringements identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. Each of the infringements concern the personal data of tens of millions of Facebook users. Further, both infringements contributed to a higher risk of fraud, impersonation and spamming in respect of the data subjects. Reprimands are appropriate in respect of such non-compliance in order to formally recognise the serious nature of the infringements and to dissuade such non-compliance.

203. The reprimand is necessary and proportionate in addition to the order in this Decision. While the order will require specific remedial action on the part of MPIL, the reprimand formally recognises the serious nature of these infringements. I consider that it is appropriate to formally recognise the serious nature of the infringements with a reprimand in order to deter future similar non-compliance by MPIL and other controllers or processors carrying out similar processing operations. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that MPIL and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations on data protection by design and by default.

N. ADMINISTRATIVE FINES

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

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

205. Article 83(2) repeats this point in stating:

> *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2).*

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

207. Article 83(1) GDPR provides:

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

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

> *(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *(g) the categories of personal data affected by the infringement;*
>
> *(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*

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

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

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

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

210. In applying the Article 83(2)(a) to (k) factors to the infringements, I have set out below my analysis of the infringements collectively, where it is possible to do so. However, in some instances it is necessary to set out each infringement individually in order to reflect the specific circumstances of each infringement and the factors falling for consideration. Regardless of whether the analysis below is individual or collective in respect of a particular factor or infringement, I have considered the infringement of Article 25(1) and the infringement of Article 25(2) separately when deciding whether to impose an administrative fine in respect of each infringement. I have made a separate decision on each infringement, and I have made each decision without prejudice to any factors arising in respect of the other infringement. For the avoidance of doubt, my decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine where applicable, is independent and specific to the circumstances of each particular infringement.

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

211. In considering the nature, gravity and duration of MPIL's infringements, I have had regard to the analysis in this Decision concerning the nature, scope, context and purposes of the processing. Article 83(2)(a) requires that I take these matters into account in having regard to the nature, gravity and duration of the infringements. Article 83(2)(a) also requires me to take into account the number of data subjects affected by the infringements and the level of damage suffered by them. Therefore, I will first consider these issues before proceeding to consider the nature, gravity and duration of the infringements.

212. MPIL indicated that the scraped dataset contained the personal data of approximately 533 million Facebook users worldwide. The analysis submitted by MPIL identified [redacted] unique UIDs belonging to data subjects from within countries of the EU. MPIL's infringement of Article 25(1) affected each of those data subjects because the appropriate technical and organisational measures that MPIL failed to implement ought

to have been in place in order to protect the rights and freedoms of each of those data subjects. The failure to implement the necessary safeguards in an effective manner at the appropriate time led to the possibility that phone numbers and email addresses could be targeted for fraud, impersonation and spamming.

213. MPIL's infringement of Article 25(2) affected each of the data subjects because MPIL failed to ensure that, by default, only personal data which are necessary for each specific purpose of the processing were processed and that by default personal data are not made accessible without the data subjects' intervention to an indefinite number of natural persons.

214. In assessing the level of damage suffered by the data subjects, I have had regard to how the infringements increased the risks posed by the processing to the rights and freedoms of Facebook users. These risks include spamming, scamming, phishing and smishing. I have had regard to the loss of control suffered by them over their personal data. A core element of the principle of data protection by default in Article 25(2) requires controllers to ensure that they only process personal data that are necessary for each specific purpose. Data subjects are denied control over their personal data where their personal data is processed in a manner that is not necessary in relation the purposes of the processing and where by default their personal data are made accessible without their intervention to an indefinite number of natural persons.

215. I find that MPIL's infringements of Article 25(2) prevented the Facebook users from exercising control over their personal data. By setting the searchability settings for users regarding the Relevant Features automatically to include each user's phone number and email address, MPIL made that personal data accessible without the individual's intervention to an indefinite number of natural persons. This intrinsically denied those data subjects control over their personal data by extending the scope of processing beyond what was necessary in relation to the purposes. Therefore, I find that this loss of control represents a significant amount of damage to the data subjects.

The Nature of the Infringements

216. Article 83(4)(a) GDPR is directed to the maximum fine that may be imposed in a particular case that involves infringement of "*the obligations of the controller and processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43*".

217. The nature of MPIL's infringements of Article 25(1) concern its failure to implement appropriate measures designed to implement the principles provided for in Article 5(1)(b) and (f) GDPR in an effective manner; and to integrate the necessary safeguards. Having regard to the nature and scope of the data processing, I consider that this failure to implement appropriate measures by design to be serious.

218. The nature of MPIL's infringement of Article 25(2) concerns its failure to ensure, using appropriate technical and organisational measures, that its processing of personal data was limited to what was necessary in relation to the purposes of that processing and the failure to ensure that by default personal data were not made accessible without the individual's intervention to an indefinite number of natural persons. MPIL's processing resulted in Facebook users' personal data being publicly available to an

indefinite and unrestricted global audience. In light of the scope of the potential audience, I find that the nature of the infringement is serious.

The Gravity of the Infringements

219. In assessing the gravity of the infringements, I have had regard to the number of data subjects affected and the level of damage suffered by them. I have also had regard to how the infringements increased the risks posed by the processing to the rights and freedoms of Facebook users. These risks include spamming, scamming, phishing and smishing. MPIL's own [redacted] highlighted the dangers arising from stalkers and burglars as a result of the disclosure of location information. MPIL submitted that 'City of Residence' was present in the scraped dataset for any data subjects who had populated that field, as it had been set to public since 18 March 2011 and had not been modified since.[124] I find that the manner in which MPIL's infringements increased the risks posed to Facebook users is highly relevant when assessing the gravity of the infringements.

220. MPIL submitted that:

> *Article 83 GDPR does not appear to contemplate that the existence of mere risks to users should even be factored into the assessment of the "nature, gravity and duration of the infringement" under Article 83(2)(a). Rather, Article 83(2)(a) states that the assessment should be based on "the level of damage suffered by them" – i.e., actual damage that has in fact occurred, as opposed to a hypothetical (and nominal) risk of future harm occurring. In relying on the latter, the PDD conflates the assessment that must be carried out pursuant to Article 25(1) GDPR, where "risks" of varying likelihood and severity for rights must be taken into account, with the assessment under Article 83(2)(a) GDPR, where only "damage suffered" is a relevant factor. The different terminology used in each article must be presumed to have a different intended meaning.*[125]

221. First as stated above, in the premises, I do not accept that the infringement can be classified as a "*mere risk*". Second, this ignores the actual wording of Article 83(2)(a) which states:

> *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;* [emphasis added]

222. The GDPR's objectives include protecting the fundamental rights and freedoms of natural persons. If an infringement of the GDPR increases the risk posed to those rights and freedoms, I must have regard to that increased risk when assessing the gravity of that infringement. 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 have not assumed or taken into account the potential existence of such damage for the purposes of this decision. However, I find

[124] Appendix D.4c at 4.

[125] Appendix D.11c at [24.3].

that in assessing the level of damage for the purpose of Article 83(2)(a), and the gravity of the infringements, it is therefore appropriate that I have regard to the likely level of damage suffered by data subjects (including non-material damage).

223. While MPIL asserts that there has been a "*conflation*" of the risks to be determined under Article 25 and the nature, gravity and duration of the infringement under Article 83(2)(a), plainly the risk to rights is intimately and closely connected to the nature, gravity and duration of the infringement and separating them would be entirely artificial. It is worth noting too that MPIL appears to be content with this conflation with its submissions in this regard.[126] Accordingly, I have also had regard to the response of MPIL and to the report of [redacted], referred to above, as they relate to the MPIL's rejection that the risk posed to data subjects was high or severe with regard to the application of Article 83(2)(a) in full. For all of the reasons set out in detail above as they relate to the specific issues that both MPIL and [redacted] raise, I remain of the view that there were high and severe risks with regard to Article 83(2)(a) *mutatis mutandis.*

224. I have assessed the gravity of MPIL's infringement of Article 25(1) in light of how it resulted in MPIL's failure to identify and to implement appropriate measures in respect of the processing to ensure compliance with the GDPR by design and to protect the rights of the data subjects. By failing to implement appropriate measures, MPIL increased the risk posed by the processing to the rights and freedoms of those data subjects. I find that the gravity of MPIL's infringement of Article 25(1) is serious.

225. In assessing the gravity of MPIL's infringement of 25(2) regarding the processing, I have had regard to how MPIL set the searchability settings for users regarding the Relevant Features automatically to include each user's phone number and email address by default. Therefore, the infringement affected approximately [redacted] data subjects in the EU. I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those users from exercising control over their personal data. The infringement also increased the risk posed to the rights and freedoms of those data subjects. The manner of processing due to the default settings resulted users' personal data being made available to an indefinite and unrestricted global audience. In those circumstances, I find that the gravity of MPIL's failure to ensure that its processing of personal data was limited to what is necessary in relation to the purpose of the processing is serious.

The Duration of the Infringements

226. The duration of MPIL's infringements of Article 25(1) regarding the processing commenced at the application of the GDPR on 25 May 2018. The obligation to implement the appropriate measures required by those articles applied from 25 May 2018. The infringement was ongoing during the period of the Temporal Scope. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement under 25(1) GDPR lasted at least from 25 May 2018 until September 2019.

[126] Appendix D.11c at [24.5]—[24.7].

227. The duration of MPIL's infringement of Article 25(2) regarding the processing commenced at the application of the GDPR on 25 May 2018. MPIL's practice of setting the searchability settings for users regarding the Relevant Features automatically to include each user's phone number and email address was in place prior to that date. Therefore, it failed to ensure that its processing of user personal data was limited to what was necessary for the specific purposes and failed to ensure that by default personal data were not made accessible without the data subjects' intervention to an indefinite number of natural persons since 25 May 2018. This infringement was ongoing during the period of the Temporal Scope and remains ongoing. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement under 25(2) GDPR lasted at least from 25 May 2018 until September 2019.

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

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

> *In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*[127]

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

> *The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.*[128]

230. In determining whether an infringement was intentional, I must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration. In determining whether an infringement was negligent, I must determine whether, despite there being no knowledge and wilfulness in respect of the characteristics of the infringement, the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

231. MPIL's infringement of Article 25(1) regarding the processing concerns its failure to implement appropriate measures to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing. Hence, the characteristics of this infringement concern that lack of appropriate technical and

[127] Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' at 11.

[128] Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' at 12.

organisational measures for the duration of the infringement. In order to classify these infringements as intentional, I must be satisfied that (i) MPIL wilfully omitted to implement appropriate technical and organisational measures and (ii) that it knew at the time that the measures that it implemented were not sufficient to meet the standards required by Article 25(1).

232. Having considered the objective elements of MPIL's conduct, as set out above, I do not consider that MPIL wilfully omitted to implement appropriate measures. While MPIL's attempts to implement appropriate measures were not sufficient for the purposes of Article 25(1), I do not consider that this failure was wilful on MPIL's part.

233. However, I consider that MPIL ought to have been aware that it was falling short of the duty owed under Article 25(1). I find that MPIL's failure to implement appropriate measures pursuant to Article 25(1) in respect of its processing was negligent in the circumstances.

234. In its submissions of 14 July 2022, MPIL stated:

> *The PDD's assertion that MPIL "ought to have been aware" that it was "falling short of the duty owed under Article 25(1)" is further problematic in that there was no guidance during the Temporal Scope indicating that controllers even had a "duty" under Article 25(1) to prevent scraping, let alone explaining how they were expected to fulfil such a duty.*[129]

And that:

> *Accordingly, the PDD's assertion that MPIL should have known it was infringing Article 25(1) during the Temporal Scope is unfounded. The PDD instead is essentially applying a strict liability standard, despite accepting that it should not, and penalising MPIL merely based on the fact that scraping occurred, rather than identifying a valid basis for any finding of negligence.*[130]

235. I do not find MPIL's above submissions persuasive. MPIL has an obligation under Article 25(1) to implement appropriate technical and organisational measures and, for the reasons set out above, I have determined it did not do so. The GDPR is a principle-based legislative measure; there is no basis for stating that it should have descriptively set out there was an obligation to prevent scraping. As set out above, a range of alternative measures were open to MPIL, which it chose not to pursue. I find that MPIL's failure to implement appropriate measures pursuant to Article 25(1) in respect of its processing was negligent in the circumstances.

236. MPIL's infringement of Article 25(2) regarding the processing concerns its failure to ensure, using appropriate technical and organisational measures, that its processing of personal data was limited to what was necessary in relation to the purposes of the processing, and that that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. Hence, the characteristics of this infringement concern MPIL's failure to implement appropriate

[129] Appendix D.11c at [25.3].

[130] Appendix D.11c at [25.4].

measures to ensure that Facebook user personal data was not made accessible (without the user's intervention) to an indefinite number of natural persons by default. In order to classify these infringements as intentional, I must be satisfied that (i) MPIL wilfully set the searchability settings for users regarding the Relevant Features to automatically include each user's phone number and email address by default in a manner that amounted to an inappropriate technical and organisational security measure (i.e. that it would expose the personal data to scrapers, who could potentially access it using reverse-lookup functionality), and (ii) that it knew at the time that this would result in personal data processing that was not limited to what was necessary in relation to the purposes and would expose the phone numbers and email addresses to processing by scrapers. In making this determination, I must rely on objective elements of MPIL's conduct that show the presence or absence of wilfulness and knowledge.

237. Having considered the objective elements of MPIL's conduct, as set out above, it is clear that MPIL wilfully set the searchability settings for users regarding the Relevant Features to automatically include each user's phone number and email address by default. MPIL has submitted that its decision to make the default searchability setting "Everyone" was not an arbitrary decision and that it reflects a core value of Facebook. I do not consider that MPIL knew at the time that this would be an inappropriate technical and organisational measure, regardless of the fact that it would, by default make the phone numbers and email addresses accessible without the data subjects' intervention to an indefinite number of natural persons. I have had regard to how the Relevant Features were not intended to return phone numbers or email addresses that were not already known to the user inputting the information, and the measures implemented by MPIL to attempt to prevent this. Having regard to these objective elements of MPIL's conduct, despite that the measures were not appropriate, I do not consider that MPIL knew at the relevant time that setting the searchability settings to "Everyone" by default would amount to an inappropriate technical or organisational measure even though it would make the phone numbers and email addresses accessible to an indefinite number of natural persons. In arriving at these conclusions, I consider that there is no evidence that MPIL acted with knowledge or wilfulness in relation to the exposure of personal data to scrapers through the Relevant Features.

238. However, I consider that MPIL ought to have been aware that it was falling short of the duty owed under Article 25(2). I find that MPIL's failure to implement appropriate measures pursuant to Article 25(2) to ensure that the phone numbers and email addresses were not made accessible without the data subjects' intervention to an indefinite number of natural persons in respect of its processing was negligent in the circumstances.

239. I consider that the that it is appropriate for me to treat the negligent character of the infringements of Article 25(1) and (2) as an aggravating factor for the purpose of this Article 83(2)(b) assessment in the circumstances of this particular inquiry, but to attribute medium weight to it when doing so in light of how these infringements were not intentional.

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

240. This Decision outlines the mitigating measures that MPIL put in place after it discovered the data scraping issue. Once appropriate measures were fully implemented, the particular scraping vector was mitigated. However, it is not always possible to retrospectively correct a past lack of control, as personal data has already been published and data subjects may already have suffered consequential damage as a result.

241. I note that the above actions by MPIL may have reduced the probability of further mass scraping causing additional risk of damage to data subjects after the infringements occurred. Having regard to these actions for the purpose Article 83(2)(c), I am of the view that the actions provided limited mitigation of the damage to data subjects, and accordingly I consider that the actions are of moderate mitigating value.

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

242. The Administrative Fines Guidelines set out that:

> *The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.*[131]

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

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

244. No relevant previous infringements arise for consideration in this context.

245. MPIL has submitted that the DPC should factor in some discount for mitigation for this. Having regard to the temporal scope, in circumstances, I consider that minimal mitigating weight attaches to this factor.

[131] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' at 13.

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

246. While I consider that the measures introduced by MPIL mitigated the data scraping issue, I note that it is not possible to fully remediate the adverse effects on Facebook users (in terms of the previous lack of control over personal data). I make this finding without prejudice to the question of whether MPIL's ongoing processing complies with the GDPR.

247. Having regard to these measures for the purpose Articles 83(2)(f) GDPR, I am of the view that the actions taken restricted further scraping to an extent. However, MPIL has not demonstrated any significant mitigation to address the possible adverse effects of the previous scraping. I consider that this factor carries moderate weight in mitigation in the circumstances.

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

248. The categories of personal data scraped from the Facebook platform included mobile phone number, name, gender, location, occupation and marital status. These personal data, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft and fraud.

249. MPIL submitted that "*'location' data was not affected, as that term is ordinarily understood, but rather the only information in the Scraped Data Set pertaining to location was hometown or city of residence*" and that " *'occupation' data was not affected, only a user's workplace was (where users chose to make it publicly viewable), which does not necessarily reveal their occupation*".[132] I accept that a user's live or precise location data was not impacted by the scraping. I also accept that a user's occupation was impacted only to the extent that this could be inferred by their workplace.

250. Social media content is typically personal to the user who posts information, including a wide range of information about a person's life and links to other people. Social media content published on a public account can therefore involve an extensive range of categories of personal data, to the extent that this activity involves the use of a largely unrestricted platform by millions of users. I am accordingly satisfied that I have properly had regard to the categories of personal data affected. Where an account was set to public, which all accounts were by default, it would have been possible for the scrapers to combine the scraped data with this personal data, thus increasing the risk of theft and fraud. This is particularly aggravating in circumstances where it was possible to combine the personal data with the scraped phone numbers that were not made public by the data subjects. In those circumstances, I consider that the categories of personal data affected by the infringements are significantly aggravating.

[132] Appendix D.11c at [30.1].

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

251. The infringements became known to the DPC as a result of multiple media reports in April 2021 which highlighted that a collated dataset of Facebook user personal data had been made available on the internet. This dataset was reported to contain personal data relating to approximately 533 million Facebook users worldwide.

252. Facebook, as it then was, engaged with the DPC on the matter in April 2021. I consider that moderate mitigating weight attaches to this factor in the circumstances.

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

253. Corrective powers have not previously been ordered against MPIL with regard to the subject matter of this Decision. This is neither an aggravating nor a mitigating factor in the circumstances.

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

254. Such considerations do not arise in this case. This is neither an aggravating nor a mitigating factor in the circumstances.

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

255. In response to the Preliminary Draft Decision on 14 July 2022, MPIL disclosed, primarily in footnotes, that that material aspects of numerous of its previous submissions were inaccurate.[133] MPIL stated that in its submissions of August 2021 and April 2022 reference was made to Messenger Contact Importer rather than Messenger Contact Creator. This late disclosure, over a year on from MPIL's initial engagement with the DPC, significantly undermined the manner in which MPIL engaged with the inquiry and the extent to which its submissions were materially erroneous. Despite lengthy submissions of 14 July 2022, MPIL did not elaborate on this fundamental error further. Complete candour by data controllers and processers when in engaging with the supervisory authority is critical to the proper application of the GDPR.

256. On 26 July 2022, as a result of this, in order to progress the inquiry and to ensure that MPIL had an opportunity to fairly clarify all errors it made, MPIL was provided with a further period within which to clarify the errors that had arisen and to explain how they had arisen, and a number of queries were put to it.

[133] Appendix D.11c at footnotes 10, 11 and 12 and at [6.11].

257. On 11 August 2022, MPIL provided its explanation for these errors as well as redlined and updated versions of its previous submissions. MPIL also took the opportunity to redline and amend its most recent submissions of 14 July 2022.

258. MPIL stated that while it and its legal advisors, including teams from two law firms, (referred to as the "investigative team") had conducted an "*extensive engagement with more than 80 stakeholders, including engineers and subject-matter experts, across more than 30 teams*", "[the] *error was inadvertent and was only discovered in the course of preparing the Response.*"[134]

259. In response to the DPC's query as to what team(s) were engaged to provide and verify the content of the erroneous submissions, MPIL stated that:

> [T]*he investigative team undertook an extensive and global effort to gather information relevant to the Inquiry and confirm that the matters presented to the DPC were accurate. This effort was supported by subject-matter experts across numerous teams, which MPIL engaged throughout the Inquiry to understand and analyse the relevant issues and to review each of the submissions presented to the DPC. The investigative team engaged with more than 80 engineers and other subject-matter experts in order to understand and analyse the issues relating to the Inquiry, including the circumstances of the scraping incidents, whose input supported the drafts of MPIL's submissions.*
>
> *Each of MPIL's submissions, drafted based on the information learned from the investigation, underwent an extensive internal review process within MPIL before being finalised and provided to the DPC. This process involved review and approval from stakeholders and subject-matter experts to confirm the accuracy of the information provided within the submissions. Throughout the Inquiry, MPIL engaged with more than 30 teams to provide and/or verify the content of the submissions that were made to the DPC in this Inquiry, including key personnel and leaders within the following teams:*
>
> ● *Abusive Account Detection;*
> ● *Anti-Scraping / External Data Misuse;*
> ● *Infrastructure teams;*
> ● *Product teams across Facebook, Instagram, and Messenger, including those dealing with messaging and search, as well as growth, integrity, and management teams;*
> ● *Privacy teams, including privacy-focused engineering, product, policy, and incident response*
> *teams; and*
> ● *Public Policy.*

260. By way of explanation for the errors, MPIL stated:

[134] Appendix D.12b at 1 and 2.

> *As reflected in MPIL's earliest correspondence with the DPC, MPIL believed at the outset of the Inquiry that Messenger CI was likely used in compiling the Scraped Data Set. This belief was based on the apparent date range of the records in the Scraped Data Set stopping in September 2019, which coincides with when Messenger CI was modified to return only friend suggestions and not direct contact matches. As far as the investigative team was aware, all other Facebook and Messenger search and contact importation surfaces had been modified prior to September 2019 so as not to return contact matches in response to phone numbers.[3] Thus, it was believed that Messenger CI was at least one of the features likely used to conduct the scraping that contributed to the Scraped Data Set.*[135]

261. The above paragraph included footnote 3, which stated: "*The investigative team was not aware of Messenger Contact Creator at the time. The investigative team now understands that Messenger Contact Creator was modified so as not to return contact matches in response to phone numbers in September 2019, around the same time as Messenger CI.*"

262. MPIL then stated:

> *Subsequently, in the course of MPIL's investigation, the investigative team learned of a scraping incident that had occurred in September 2018 (the "September 2018 Incident"), which it understood at the time to relate to Messenger CI. The September 2018 Incident was described as affecting Messenger contact "creation", and (in line with the belief that Messenger CI was one of the features used to assemble the Scraped Data Set) the investigative team misunderstood this to refer to Messenger CI, as Messenger CI enabled the creation of Messenger contacts through importation of a user's address book on their mobile device. The investigative team engaged extensively with engineers who had been assigned to the Anti-Scraping Team as at September 2018 about the incident, as well as engineers from the Messenger teams responsible for search and contact importation functionality on Messenger. Multiple engineers from these teams were likewise involved in reviewing the relevant sections of MPIL's submissions in the Inquiry. Unfortunately, however, no error was flagged regarding the description of the feature involved in the incident. Accordingly, the September 2018 Incident was referenced as involving Messenger CI in MPIL's August 2021 submission (at footnote 10 on page 20), and changes to certain rate limits made in response to the incident were referenced in MPIL's April 2022 submission as having been made to Messenger CI (in response to Query 1).*
>
> *It was only in June 2022, in the course of preparing the Response, that the investigative team discovered the mistake. In particular, in reviewing the rate limit modifications made in response to the September 2018 Incident, which were noted in the PDD, the investigative team learned that the rate limits applied only to lookups of single users rather than uploads of address books. This did not make sense to the investigative team given that Messenger CI facilitates the upload of*

[135] Appendix D.12b at 2.

> *address books, rather than lookups of single users. The investigative team accordingly looked into this matter further and discovered that the September 2018 incident actually involved a now defunct feature with which the investigative team was not previously familiar, known as "Messenger Contact Creator" – a variant of Messenger Search used to search for an individual user on the Messenger mobile app and add them to one's Messenger contacts, rather than a contact importation surface. Accordingly, MPIL corrected the position in the Response and provided details about the Messenger Contact Creator feature.*
>
> *In light of this discovery, the investigative team also reviewed all statements in prior submissions relating to Messenger CI, including in relation to the scraping incident discovered in August 2019, for the purposes of the Response. The investigative team had originally understood this later incident to involve scraping detected both on Messenger Search and Messenger CI, based on engagements with subject matter experts as well as the fact that mitigations taken in response to the incident covered both Messenger Search and Messenger CI. Through further investigation, the investigative team learned that the scraping actually detected in the incident occurred exclusively on Messenger Search, and that the mitigations applied to Messenger CI were made proactively. Accordingly, MPIL corrected this position in the Response as well.*[136]

263. Despite this explanation, it remains difficult to understand how such a fundamental error could have occurred over such a long period, in spite of MPIL's considerable financial and personnel resources and large number of teams, stakeholders and subject-matter experts responsible for analysing, preparing and reviewing its submissions, and that it had the benefit of the expertise of two external legal teams. Indeed, that the MPIL investigative team was not initially aware of Messenger Contact Creator is of particular note.

264. How such far-reaching inaccuracies could have been submitted to the DPC in the first instance, and how they remained undisclosed or unnoticed for so long, undermines the manner in which MPIL engaged with the DPC in the course of this inquiry.

265. The extent and seriousness of the errors were undiscovered for a lengthy period. Such errors have inevitably delayed the progress of this inquiry which itself was exacerbated by the fact that MPIL had to be given a further opportunity to clarify and elaborate on its errors in circumstances where it chose not to do so in the course of its response to the Preliminary Draft Decision. Considering all of these circumstances and that by MPIL's contention these errors arose due to inadvertence (that is, a failure to take proper care), I find that this constitutes an aggravating factor in respect of both infringements. I consider that significant weight must attach to this as an aggravating factor.

[136] Appendix D.12b at 2 to 3.

O. DECISIONS ON WHETHER TO IMPOSE ADMINISTRATIVE FINES

266. In deciding whether to impose an administrative fine in respect of each infringement, I have had regard to the factors outlined in Article 83(2)(a) – (k) GDPR cumulatively, as set out above. However, I have considered each infringement separately when applying those factors, when deciding whether to impose an administrative fine, and when deciding the amount of each administrative fine. I have also had regard to the effect of the order and reprimand in ensuring compliance with the GDPR. The order will assist in ensuring compliance by mandating specific action on the part of MPIL in order to re-establish compliance with specific findings of infringements. The reprimand will contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements. However, I consider that these measures alone are not sufficient in the circumstances to ensure compliance. I find that administrative fines in respect of each of the infringements are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

267. In order to ensure compliance with the GDPR, it is necessary to dissuade non-compliance. Depending on the circumstances of each individual case, dissuading non-compliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. Where a serious infringement of the GDPR occurs, a reprimand may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) GDPR for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 GDPR acknowledges that, depending on the circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, reprimands and other corrective powers:

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

268. While the order in this Decision will re-establish compliance with the specific infringements identified, I do not consider this measure appropriate to deter other future serious infringements. While the reprimand will assist in dissuading MPIL and other entities from similar future non-compliance, in light of the seriousness of the infringements, I do not consider that the reprimand is proportionate or effective to achieve this end. I find that administrative fines are necessary in respect of each of the infringements to deter other future serious non-compliance on the part of MPIL and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

(1) Each of the infringements are serious in nature and gravity as set out pursuant to Article 83(2)(a). Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of

other entities carrying out similar processing. Regarding the infringement of Article 25(1), in circumstances where MPIL has submitted that the public personal data of at least [redacted] data subjects within EU countries (forming part of approximately 533 million Facebook users worldwide) has been collated in the dataset, I consider that non-compliance with its obligations under this Article must be very strongly dissuaded. This is particularly the case given the nature of the personal data, including phone numbers and email addresses. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, I consider that an administrative fine is appropriate and necessary in the circumstances.

(2) Regarding MPIL's infringement of Article 25(2), processing of user personal data in a manner that is not limited to what is necessary in relation to the purposes of that processing must be strongly dissuaded. By setting the searchability settings for users regarding the Relevant Features automatically to include each user's phone number and email address, MPIL made that personal data accessible without the individual's intervention to an indefinite number of natural persons and therefore exposed the data subjects to the risks of fraud, scamming and impersonation. Given that such activities constitute a high risk to the rights and freedoms of natural persons, which could lead to physical, material or non-material damage, I consider that an administrative fine is appropriate and necessary in order to dissuade non-compliance.

(3) Having regard to the nature, gravity and duration of the infringements, I also consider that administrative fines are proportionate in the circumstances in view of ensuring compliance. The loss of control suffered by the data subjects as a result of MPIL's infringement of Article 25(2) affected approximately [redacted] data subjects in the EU. MPIL has not identified the number of non-EU EEA data subjects affected. I consider that the loss of control over personal data constitutes significant damage in the circumstances. The infringement of Article 25(2) is ongoing. In light of this damage, and how it was suffered by a significant number of users, I consider that fines are proportionate to responding to MPIL's particular infringement of Article 25(2) with a view to ensuring future compliance. Again, the nature of the personal data at issue is also relevant here. I consider that fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

(4) I consider that the negligent character of MPIL's infringements of Article 25(1) and (2) carries weight when considering whether to impose administrative fines, and if so, the amount of those fines. While I do not consider that MPIL wilfully omitted to implement appropriate measures, MPIL's attempts to implement appropriate measures were not sufficient for the purposes of Article 25(1), and it is clear that MPIL ought to have been aware that it was falling short of the duty owed under Article 25(1). Furthermore, I consider that MPIL was negligent and ought to have been aware of its failure to implement appropriate measures pursuant to Article 25(2) to ensure that the phone numbers and email addresses were not made accessible without the data subjects' intervention to an indefinite number of natural persons. This negligence suggests that administrative fines are necessary

to effectively ensure that MPIL directs sufficient attention to its obligations under Article 25(1) and (2) in the future.

(6) I consider that administrative fines would help to ensure that MPIL and other similar controllers take the necessary action to ensure the upmost care is taken to avoid infringements of the GDPR in respect of users' data. In these particular circumstances where the categories of users' data affected by MPIL's infringements carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft and fraud, I consider that administrative fines are appropriate and dissuasive, particularly in order to counter any financial incentives that may exist for controllers and processors who may infringe the GDPR, either intentionally or negligently.

(7) I have had regard to the manner in which MPIL has engaged with this inquiry. In particular, that inaccurate information had been submitted and the explanation for same.

269. (8) I have had regard to the lack of previous relevant infringements by MPIL, which is a mitigating factor. I also had regard to the actions taken by MPIL in order to minimise further scraping (as assessed above pursuant to Articles 83(2)(c) and (f)). I consider that these factors mitigated the damage to data subjects to an extent, and remedied the infringements to an extent. I have therefore taken these mitigating actions into account when calculating the administrative fines. However, despite these factors, I consider that administrative fines are appropriate, necessary and proportionate in respect of each infringement in order to ensure compliance with the GDPR. While the lack of previous relevant infringements is a mitigating factor, I consider that the need to dissuade non-compliance of this nature concerning the personal data of millions of data subjects far outweighs the mitigation applied for this factor. I note that the data subjects affected may include children and vulnerable people. Furthermore, despite the actions taken to mitigate against further scraping by the same method, the damage suffered as a result of the infringements has not been significantly mitigated for the affected data subjects. In light of the negligent character of the infringements, and MPIL's failure to comply with its obligations with regard to data protection by design and default, I consider that dissuasive administrative fines are necessary in the circumstances to ensure future compliance. Based on the analysis I have set out above, I have decided to impose the following administrative fines:

(1) In respect of MPIL's infringement of Article 25(1) GDPR regarding the processing (Finding 1), I have decided to impose a fine of €150 million.

(2) In respect of MPIL's infringement of Article 25(2) GDPR regarding the processing (Finding 2), I have decided to impose a fine of €115 million.

270. I have taken into account – in accordance with the approach of the EDPB – Facebook, Inc's turnover as set out below in my calculation of the appropriate amount of the administrative fines. I consider that it is appropriate to do so in order to ensure that the administrative fines satisfy the requirement in Article 83(1) GDPR for any administrative fine imposed to be effective, proportionate and dissuasive in each individual case.

271. In its submissions of 14 July 2022, MPIL stated:

> *The DPC has taken account of turnover in the determination of the level of administrative fines in a manner that is incorrect. This is not specified as a factor to which regard is to be had in Article 83(2) GDPR. Nevertheless, the PDD at paragraph 212 states that the EDPB's decision relating to IN 18-12-2, an inquiry conducted by the DPC into WhatsApp Ireland Limited's compliance with Articles 12, 13 and 14 GDPR ("Decision 1/2021") "directed the DPC to take account of the undertaking's turnover in the calculation of the fine amounts and I therefore factor that turnover figure below into my calculation of the individual infringement finding ranges".*[137]

272. This submission suggests that taking into account of the undertaking's turnover is incorrect as a matter of law, as it is not set out as a factor in Article 83(2) GDPR. In this regard, the DPC relies on its existing analysis of its obligations to cooperate with the concerned supervisory authorities and apply the GDPR consistently. As in the EDPB Decision concerning WhatsApp, the DPC intends to maintain this consideration of the undertaking's turnover pursuant to Article 83(1) GDPR. The EDPB determined in its decision 1/2021 that: [138]

> *…the EDPB takes the view that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR.*[139]

273. In having determined the quantum of the fines above, I have taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be *effective, proportionate and dissuasive* in each individual case.

274. My view is that, in order for any fine to be *effective*, it must reflect the circumstances of the individual case. As outlined above, the infringements are all serious in nature and in gravity. The infringements concern the personal data of Facebook users and the infringements all increased the risks posed by the processing to the right and freedoms of those data subjects, in particular in relation to the risk of fraud, impersonation, and spamming. In order for a fine to be *dissuasive*, it must dissuade both the controller/processor concerned, as well as other controllers or processors carrying out similar processing operations, from repeating the conduct concerned. As regards the requirement for any fine to be *proportionate*, this requires me to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR.

275. In this regard, MPIL has submitted that:

[137] Appendix D,.11c at [34.1].

[138] 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

[139] Ibid at paragraph 412.

> *The PDD applies a cursory analysis to the requirement that an administrative fine be "effective", which the DPC acknowledges "must reflect the circumstances of the individual case", and relies almost entirely on its flawed assessment that the infringements were "serious in nature and in gravity" and that such infringements increased risks posed to data subjects.* […]
>
> *The proposed fines, both individually and cumulatively, are disproportionate and go far beyond what is required to be "dissuasive" considering the circumstances of the Inquiry. This is evidenced by the good faith efforts taken by MPIL to comply with Article 25 GDPR at the time of the processing and the numerous mitigating measures that were implemented by MPIL in respect of the processing* […].
>
> *Finally, the proposed fines, both individually and cumulatively, are not proportionate to the circumstances of the Inquiry because they individually and in totality far exceed the minimum amount necessary to achieve the objectives pursued by the GDPR. It is a fundamental principle of EU law that the DPC must impose the least onerous measures available to it. While MPIL does not consider any administrative fine is warranted, in order to satisfy this criterion, any such fine must correspond to the minimum amount necessary to ensure compliance with the GDPR. MPIL submits that the proposed fines far exceed the minimum necessary. The disproportionate nature of the proposed fines is further highlighted by the lack of due regard given to the fact that MPIL has addressed the alleged infringements and that in any event a reprimand and an order to bring processing into compliance is also being proposed.*[140]

276. I do not accept this submission. This Decision has engaged in lengthy analysis both with regard to the substance of the infringements under Article 25, as well as a detailed examination of the factors that arise under all aspects of Article 83(2) and (3). This Decision has engaged with the submissions provided by MPIL, and has given consideration of the efforts made by MPIL. This is all set out exhaustively in this Decision.

277. I am satisfied that the fines above do not exceed what is necessary to enforce compliance with the GDPR taking into account the size of MPIL's user base, the loss of control over personal data suffered by the data subjects, and how infringements increased the risks posed by the processing to the right and freedoms of the data subjects.

278. I am satisfied that the two ranges for the fines specified above would be effective, proportionate and dissuasive, taking into account all of the circumstances of this Inquiry.

<u>O.1 Article 83(3) & (4)</u>

279. Having completed my assessment of whether or not to impose a fine (and of the amount of any such fine), I must now consider the remaining provisions of Article 83

[140] Appendix D.11c at [37.3].

GDPR, with a view to ascertaining if there are any factors that might require the adjustment of the fines.

280. 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.*

281. The European Data Protection Board ('**the EDPB**') adopted a binding decision ('**the EDPB Decision concerning WhatsApp**')[141] relating to IN-18-12-2, an Inquiry conducted by the DPC into WhatsApp Ireland Limited's compliance with Articles 12, 13 and 14 GDPR. The EDPB Decision concerning WhatsApp arose out of a dispute resolution procedure pursuant to Article 65 GDPR, and was adopted by the DPC in conjunction with the DPC's final decision on 2 September 2021.

282. In light of the DPC's obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR, it is necessary for me to follow the EDPB's interpretation of Article 83(3) GDPR in inquiries given that it is a matter of general interpretation that is not specific to the facts of the case in which it arose.

283. The relevant passage of the EDPB decision concerning WhatsApp is as follows:

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

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

not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.

318. *In this case, the issue that the EDPB is called upon to decide is how the calculation of the fine is influenced by the finding of several infringements under Article 83(3) GDPR.*

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

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

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

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

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

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

> *effective, proportionate and dissuasive within the limit of the gravest infringement". The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.*
>
> *325. The wording "total amount" also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording "total amount" in this regard already implies that other infringements have to be taken into account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.*
>
> *326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.*
>
> *327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiven*ess.

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

285. MPIL has made discrete submissions that require consideration. First, that it does not accept the EDPB's interpretation *per se*,[142] second, that the EDPB's decision is not binding,[143] and third, that (even if it were binding) it has not been correctly applied in the present inquiry.[144]

286. In relation to the first, I do not accept the MPIL contention that the EDPB is incorrect in its interpretation. I endorse and agree with the reasoning set out by the EDPB at [315]-[326] of the EDPB decision concerning WhatsApp, quoted above.

[142] Appendix D.11c at [35.1]-[35.3].

[143] Appendix D.11c at [35.4]-[35.11].

[144] Appendix D.11c at [35.12]-[35.17].

287. In relation to the second, regardless of whether or not the EDPB Decision is binding, its *interpretation* is correct in law and accordingly has been applied here having regard to the individual factors of the inquiry.

288. In relation to the third, MPIL states:

> *a) First, Decision 1/2021 expressly confirms the application of Article 83(3) GDPR is subject to the overarching requirement that the fine comply with Article 83(1) GDPR. While Decision 1/2021 notes that "several amounts can be determined" in the event of several infringements, it goes on (in several places) to emphasise the importance of Article 83(1) GDPR.*
>
> *(b) Second, Decision 1/2021 requires that, where there are several infringements, "these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed". This was in response to the fact that "CSAs argued in their respective objections that not taking into account infringements other than the 'gravest infringement' is not in line with their interpretation of Article 83(3) GDPR". Accordingly, Decision 1/2021 did not direct the DPC to impose separate fines in respect of each infringement and to then add those fines together.*
>
> *Moreover, MPIL submits that the manner in which the proposed fine has been imposed offends against the Charter of Fundamental Rights and Freedoms and the general principles of EU law, in accordance with which the GDPR must be interpreted, including proportionality, legitimate expectations, ne bis in idem, and concurrency of laws. MPIL is concerned that the DPC, in seeking to comply with what it considers to be the directions of Decision 1/2021, has failed to have due regard to these principles by which it is bound when calculating the amount of the proposed fines. The fines being proposed are essentially two fines for what is essentially the same set of facts and the same alleged infringement of one GDPR provision, namely Article 25 GDPR. MPIL submits that the DPC's proposed approach amounts to double punishment for the same conduct and is inconsistent with principles regarding the concurrence of laws, in accordance with which fines may not be applied cumulatively in respect of the same or linked conduct.*
>
> *There is significant – if not complete – overlap between the infringements. The underlying conduct is identical and the infringements are one and the same. The DPC does not go on to take into account the overlapping nature of the infringements at all in the analysis on fines.* [145]

289. I do not accept MPIL's submissions in this regard. This Decision has separately set out the reasons for the infringements of Article 25(1) and 25(2) respectively. While both infringements relate to the Relevant Features during the Temporal Scope, the conduct relating to the separate infringements is distinct and this conduct does not overlap.

290. The infringement of Article 25(1) concerns MPIL's failure to implement appropriate measures designed to implement the data protection principles provided for in Article

[145] Appendix D.11c at [35.14]-[35.15].

5(1)(b) and (f) GDPR. I have set out in detail how that failure to implement appropriate measures in respect of the purpose limitation principle provided for in Article 5(1)(b) GDPR exposed the Relevant Features to use by bad actors to create a data set, rather than finding profiles of Facebook users known to them. I have also set out in detail how that failure to also consider that MPIL failed to implement appropriate measures in respect of the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR enabled bad actors to use the Relevant Features to discover whether random combinations of numbers and letters correspond to valid phone numbers and email addresses, and, if so, to discover the identity of the Facebook user who owns the relevant phone number or email address. This is the basis for the infringement of Article 25(1) GDPR. This infringement does not relate to whether the searchability settings for users regarding the Relevant Features were automatically set to include each user's phone number and email address. Regardless of whether their inclusion was by default or by active choice, MPIL was obliged, pursuant to Article 25(1), to implement appropriate measures which were designed to implement the purpose limitation principle and the integrity and confidentiality principle.

291. The infringement of Article 25(2), on the other hand, concerns how the searchability settings for users regarding the Relevant Features were automatically set to include each user's phone number and email address. For the reasons already set out in this Decision, as a result of this default setting, MPIL failed to implement appropriate technical and organisational measures to ensure that, by default, only personal data which were necessary for each specific purpose of the processing were processed, and failed to ensure that by default personal data were not made accessible without the data subjects' intervention to an indefinite number of natural persons. This infringement meant that even where a user did not intervene to make their phone number and email address searchable in the Relevant Features, that phone number and email address was nonetheless searchable. This, in turn, also meant that the phone number and email address was vulnerable to scraping through the Relevant Features, even though the user had not decided to make their contact details searchable.

292. I have set out in detail the individual findings with regard both the substantive breaches of the GDPR under Article 25 and the corrective measures, as well as the reasoning for them. I have engaged in a lengthy and thorough examination of the application of both provisions within Article 25. Simply because the infringements are both to do with scraping, does not in itself mean MPIL is being doubly punished – rather for all of the reasons set out at length, the corrective measures arise for different reasons and were determined with due consideration of the overall proportionality of the overall sanctions within this decision.

293. Regarding Article 83(4) GDPR, I note that this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

294. Article 83(4) GDPR provides as follows:

> *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

> *(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;*
>
> *…*

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

> *Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.*[146]

296. Accordingly, when considering a respondent's status as an undertaking, the GDPR requires me to do so by reference to the concept of *'undertaking'*, as that term is understood in a competition law context. In this regard, the Court of Justice of the European Union ('**the CJEU**') has established that:

> *an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed*[147]

297. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement.[148]

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

299. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the

[146] Treaty on the Functioning of the European Union.

[147] Judgment of 23 April 1991, *Höfner and Elser v Macrotron GmbH*, Case C-41/90, EU:C:1991:161, at [21].

[148] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, Case C-97/08 P, EU:C:2009:536, at [58]-[60].

economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case.[149]

300. The CJEU has, however, established[150] that, where a parent company has a 100% shareholding in a subsidiary, it follows that: the parent company is able to exercise decisive influence over the conduct of the subsidiary; and a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

301. The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary.[151]

302. The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise decisive influence over the conduct of its subsidiary.[152] This reflects the position that:

> *… the presumption of actual exercise of decisive influence is based, in essence, on the premise that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day business of that subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company …*[153]

303. Where the presumption of decisive influence has been raised, it may be rebutted by the production of sufficient evidence that shows, by reference to the economic, organisational and legal links between the two entities, that the subsidiary acts independently on the market.

304. It is important to note that 'decisive influence', in this context, refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR,

[149] Judgment of 14 September 2016, *Ori Martin and SLM v Commission*, C-490/15 P, ECLI:EU:C:2016:678,at [60].

[150] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:536.

[151] Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, at [48].

[152] Judgment of 7 June 2011, *Total and Elf Aquitaine v Commission*, T-206/06, not published, EU:T:2011:250, at [56]; Judgment of 12 December 2014, *Repsol Lubricantes y Especialidades and Others v Commission*, T-562/08, not published, EU:T:2014:1078, at [42]; Judgment of 15 July 2015, *Socitrel and Companhia Previdente v Commission*, T-413/10 and T-414/10, EU:T:2015:500, at [204].

[153] Opinion of Advocate General Kokott in *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:262, point 73. Cited in Judgment of 12 July 2018, *The Goldman Sachs Group, Inc. v European Commission*, Case T-419/14, ECLI:EU:T:2018:445, at [51].

in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.

305. As noted above, within the European Region, the Facebook service is provided by a subsidiary of Meta Platforms, Inc. previously known as Facebook Ireland Limited and now known as Meta Platforms Ireland Limited (referred to as '**MPIL**' in this Decision). MPIL's ultimate parent is Meta Platforms, Inc.

306. I have had regard to MPIL's Directors' Report and Financial Statements[154] for the Financial Year ended 31 December 2020, which are available from the Companies Registration Office and are dated October 2021. On page 3 of the document, it is stated that:

> *Facebook Ireland Limited is wholly owned by Facebook International Operations Limited, a company incorporated in the Republic of Ireland. Its ultimate holding company and controlling party is Facebook, Inc., a company incorporated in the United States of America.*

307. At Note 24 to the Financial Statements, on page 41, it is stated that:

> *At 31 December 2020, the company is a wholly-owned subsidiary of Facebook International Operations Limited, a company incorporated in the Republic of Ireland, its registered office being 4 Grand Canal Square, Grand Canal Harbour, Dublin 2.*
>
> *The ultimate holding company and ultimate controlling party is Facebook, Inc., a company incorporated in Wilmington, Delaware, USA. The ultimate holding company and controlling party of the smallest and largest group of which the company is a member, and for which consolidated financial statements are drawn up, is Facebook, Inc.*

308. For the purpose of the Preliminary Draft Decision, I had assumed that the above has remained the position in the interim. I note, in this connection, that the same position was stated in MPIL's Directors' Report and Financial Statements for the year ended 31 December 2019, which is dated December 2020. I also note in relation to the above that Facebook, Inc. changed its name to Meta Platforms, Inc. as of 28 October 2021.

309. On this basis, it was my understanding that MPIL is a wholly-owned subsidiary of Facebook International Operations Limited; Facebook International Operations Limited is wholly owned and controlled by Meta Platforms, Inc.; and, as regards any intermediary companies in the corporate chain, between MPIL and Meta Platforms Inc., it is assumed, by reference to the statement at Note 24 of the Notes to the Financial Statements (quoted above) that the "*ultimate holding company and controlling party of the smallest and largest group of which* [MPIL] *is a member … is Facebook, Inc.* [now Meta Platforms, Inc.]". It was, for the purposes of the Preliminary Draft Decision, therefore assumed that Meta Platforms, Inc. is in a similar situation to that of a sole

[154] Appendix D.9c.

owner as regards its power to (directly or indirectly) exercise a decisive influence over the conduct of MPIL.

310. It seemed to be therefore, that the corporate structure of the entities concerned is such that Meta Platforms, Inc. is in a position to exercise decisive influence over MPIL's behaviour on the market. Accordingly, a rebuttable presumption arose to the effect that Meta Platforms, Inc. does in fact exercise a decisive influence over the conduct of MPIL on the market.

311. If this presumption is not rebutted, it would mean that Meta Platforms, Inc. and MPIL constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant *'cap'* for the purpose of Article 83(4) GDPR, would fall to be determined by reference to the combined turnover of MPIL and Meta Platforms, Inc. The Preliminary Draft Decision operated on the basis of that presumption, without prejudice to any such submissions MPIL might make in rebuttal. I have had full regard to the submissions of MPIL made in response to the Preliminary Draft Decision.

312. In this respect, MPIL made two discrete submissions on 14 July 2022. First, that Meta Platforms, Inc does not constitute the relevant "undertaking" under these provisions of the GDPR and rather MPIL does. Second, MPIL asserts that the "preceding financial year" for the purposes of the GDPR is the year preceding the relevant infringements, not the year preceding the imposition of the administrative fine.[155]

313. In relation to the first, MPIL stated that the DPC's views on the question of the relevant "undertaking" for the purposes of Articles 83(4) to (6) GDPR are wrong as a matter of fact and law.[156] MPIL provided a number of reasons why:

> *(a) 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.*
> *(b) 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.*

[155] MPIL repeatedly erroneously refers to Article 83(5) rather than Article 83(4) GDPR. I have considered MPIL's submissions in this regard as if they referred to Article 83(4) GDPR.
[156] Appendix D.11c at [36.1].

> *(c) Accordingly, in order to determine whether Meta exercises decisive influence over MPIL's "conduct on the market" for the purposes of the GDPR, the DPC's analysis should properly focus on MPIL's data processing activities and the related decision making about personal data processed by MPIL. MPIL 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.*
> *(d) Conduct under the GDPR can be attributed to multiple legal persons only if, in accordance with Article 4(7) GDPR, two or more legal persons "jointly" determine the purposes and means of the processing of personal data. Control in the economic sense is not sufficient to establish "joint controllership" within the meaning of the GDPR. Parents and subsidiaries may act as controllers and processors depending on their different functions. As is clear from Articles 24, 28 and 29 GDPR, the rules governing the relationship between the controller and the processor are identical, irrespective of whether these legal persons are part of the same group of companies or are unrelated companies.*
> *(e) As the DPC is aware, MPIL is the controller for user data processed for the purposes of providing the Facebook Service in the EEA (as well as other countries in the European region).*
> *(f) Accordingly, Meta cannot properly be said to have "decisive influence" when that term is considered in a GDPR context.*[157]

314. MPIL then stated:

> *MPIL submits that it does in fact operate with sufficient independence on the market such that it should not be conflated with Meta on the basis of an assessment of "behaviour on the market" in the context of the GDPR. In particular, as regards the Relevant Features in the EEA, MPIL is the entity responsible for:*
>
> > *(a) making the Relevant Features available to users;*
> > *(b) setting policies that govern how user data is processed and with respect to how settings are set by default;*
> > *(c) controlling access to and use of user data;*
> > *(d) handling and resolving data-related inquiries and complaints regarding the Facebook and Messenger service from users whether directly or indirectly;*
> > *(e) ensuring the Relevant Features' compliance with EU data protection laws;*
> > *(f) ongoing evaluation of the Relevant Features; and*
> > *(g) guiding the development of products involving user data in accordance with EU data protection laws.*
>
> *In light of the points set out above, MPIL's position is therefore that the relevant "undertaking" for the purpose of Articles 83(4) to (6) GDPR is MPIL alone. MPIL reserves the right to make further submissions in this regard if necessary.*[158]

[157] Appendix D.11c at [36.4].
[158] Appendix D.11c at [36.5]-[36.6].

315. I do not accept this interpretation and I do not consider that the presumption has been rebutted for the following reasons:

i. 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 purpose*s." 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 Article 83(4) to (6) GDPR.

ii. The concept of an "undertaking" in Article 101 and 102 TFEU is not defined in the text of those articles, but rather has developed by interpretation 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 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 to have done so explicitly. As it stands, there is no clear basis in the text of the GDPR for MPIL'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.

iii. 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*."[159] The CJEU has emphasised that in examining whether the parent company is able to exercise decisive influence over the

[159] Judgment of 11 July 2019, *Huhtamäki Oyj,* T-530/15, EU:T:2019:498 at [228].

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.[160] 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.[161] 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.

iv. Accordingly, the fact that MPIL 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, Meta Platforms, Inc., is necessarily rebutted.

v. MPIL 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 Meta Platforms, Inc. over MPIL's conduct on the market.

316. In relation to the second, MPIL stated that:

> *Article 83(5) GDPR refers to the relevant undertaking's turnover in the "preceding financial year". The DPC appears to presume that the relevant preceding financial year is the year preceding the imposition of the administrative fine. MPIL considers that the DPC's apparent presumption is wrong as a matter of law and submits that preceding financial year for the purposes of Articles 83(4) to (6) GDPR is the year that precedes the relevant infringement(s), or at least preceding the commencement of the investigation. This is particularly so in this Inquiry, given that the Temporal Scope, and therefore the alleged infringements in respect of which administrative fines are proposed, ended in 2019 and any final decision in the Inquiry will be made in 2022 at the earliest.*[162]

317. I do not accept this interpretation of either Article 83(4) or (5) GDPR. The interpretation does not appear to have any basis at all in those provisions. Plainly, if it were the case that the preceding financial year was that prior to the infringement rather than the determination of the administrative fine, Article 83 would state this. Per the draft EDPB Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR:

> ***Turnover is taken from the annual accounts of an undertaking, which are drawn up with reference to its business year and provide an overview of the past financial year of a company or of a group of companies (consolidated accounts).*** *Turnover is defined as the sum of all goods and services sold. The term turnover*

[160] Judgment of 11 July 2013, *Commission v. Stichting Administratiekantoor Portielje*, C-440/11 P, EU:C:2013:514 at [60] and [66].

[161] Judgment of the CJEU of 8 May 2013, *Eni v. Commission*, C-508/11, EU:C:2013:289 at [64]-[68].

[162] Appendix D.11c at [36.7].

> *within the meaning of Article 83(4)–(5) GDPR is to be understood in terms of the net turnover of Directive 2013/34/EU. According to this directive, net turnover means the amount derived from the sale of products and the provision of services after deducting sales rebates and value added tax (VAT) and other taxes directly linked to turnover.* [emphasis added] [163]

318. I calculate the administrative fine on the basis that Facebook, Inc. (as it was then called) had a reported a total revenue of $117.929 billion U.S. dollars for the year ended 31 December 2021.[164] This was an increase of 37% over the total revenue for 2020, when Facebook, Inc. had a reported total revenue of $85.965 billion U.S. dollars.

319. Applying the above to Article 83(4) GDPR, I first note that, in circumstances where the fine is being imposed on an *'undertaking'*, a fine of up to 2% (in respect of infringements of each of Article 25(1) and Article 25(2) GDPR) of the undertaking's total worldwide annual turnover of the preceding financial year may be imposed. I further note that the fines are (respectively) less than 2% of Meta Platforms, Inc.'s total worldwide annual turnover for the year 2021. That being the case, the fines above do not exceed the applicable fining 'cap' prescribed by Article 83(4) GDPR.

320. I consider that MPIL's infringement of Article 25(1) is the gravest infringement (concerning the public-by-default accessibility setting). This is for the reasons as set out above. I further note that the associated maximum possible fine for that infringement under Article 83(4) GDPR is 2% of the turnover of Meta Platforms, Inc. It is further to be noted that the EDPB's Decision concerning WhatsApp, from which I quoted above, also directed the DPC to take account of the undertaking's turnover in the calculation of the fine amounts and I therefore factor that turnover figure below into my calculations of the individual infringement fining ranges. When the amounts of the individual infringements are added together, a total figure of €265 million arises. The combined fines are also below 2% of the turnover of Meta Platforms, Inc. as required by Article 83(3) GDPR.

[163] EDPB Guideline 04/2022 on the Calculation of Administrative Fine under the GDPR (Adopted 12 May 2022) accessible via https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

[164] Appendix D.9d, Press Release, 'Facebook Reports Fourth Quarter and Full Year 2021 Results' available at https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx

P. SUMMARY OF ENVISAGED ACTION

321. In summary, the corrective powers that I shall exercise are:

(1) An order pursuant to Article 58(2)(d) GDPR to MPIL to bring its processing into compliance with the GDPR in the manner specified in this Decision. This should be done within three months of the date of notification of any final decision;

(2) A Reprimand to MPIL pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and

(3) Two administrative fines, as follows:

1. In respect of MPIL's infringement of Article 25(1) GDPR (Finding 1), I impose an administrative fine of €150 million.
2. In respect of MPIL's infringement of Article 25(2) GDPR (Finding 2), I impose an administrative fine of €115 million.

322. In having selected the specific figures, in respect of the infringements identified above, from the upper end of the fining ranges that were proposed by way of the Provisional Draft Decision, I have taken account of the following:

a. My assessment of the individual circumstances of this particular inquiry, as summarised 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 MPIL in the various submissions furnished on fining matters. I note, in this regard, that MPIL has submitted that the DPC was incorrect in law to follow the reasoning of the EDPB in the WhatsApp Ireland decision in relation to taking account of turnover in the determination of the level of administrative fines. I disagree with this suggestion. Otherwise, the manner in which I have taken account of the matters raised in MPIL's submissions is already addressed, under the relevant heading of the Article 83 assessment, above.

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

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

This Decision is addressed to:

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

Dated the 25th day of November 2022

Decision-Maker for the Commission:

____
Helen Dixon
Commissioner for Data Protection