

In the matter of the General Data Protection Regulation

DPC Inquiry Reference: IN-20-7-4

**In the matter of Meta Platforms Ireland Limited, formerly Facebook Ireland Limited, and
the “Instagram” social media network**

**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 Commission:

Helen Dixon

Commissioner for Data Protection

Dated the 2nd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

A. Introduction	1
B. Background	1
B.1 The Instagram service	1
B.2 Issues referred to Facebook by David Stier	3
B.3 Issues referred to Supervisory Authorities by David Stier	4
B.4 Introduction of “creator accounts” and modification of Instagram business accounts.....	4
B.5 Supervisory engagement between the DPC and FB-I	5
B.6 Preliminary assessment of Mr Stier’s allegations by the DPC	6
C. Commencement and Scope of Inquiry	7
C.1 Inquiry actions to date	7
C.2 Temporal scope of Inquiry	9
C.3 Material scope of Inquiry.....	9
C.4 Assessment of FB-I’s compliance with the GDPR, and consideration of corrective powers	12
D. Preliminary legal and procedural issues	14
D.1 Competence of the DPC as lead supervisory authority.....	14
D.2 Procedural issues raised by FB-I prior to the Preliminary Draft Decision.....	15
D.3 Purported DPC reliance on draft guidance.....	16
D.4 Legal, factual and procedural issues raised by FB-I concerning the DPC assessment of the <i>purpose of public by default processing</i>	18
Consideration of FB-I’s submissions on the DPC assessment of the purpose of processing.....	19
Factual assessment of the purpose of public-by-default processing	21
Procedural issues regarding the purpose of public-by-default processing	25
Preliminary conclusion on the purpose of public-by-default processing	29
D.6 Assessment of “ <i>risk</i> ” in the context of the GDPR.....	30
D.7 Purported failure on the part of the DPC to provide a “ <i>Statement of Facts</i> ”	31
E. Consideration of Article 6 GDPR	32
Compliance with Article 6(1) GDPR	32
Submissions of FB-I regarding Article 6 GDPR	32
Analysis and findings of the DPC.....	35
Assessment of processing on the basis of Article 6(1)(b) GDPR.....	35
Assessment of processing on the basis of Article 6(1)(f) GDPR.....	42
F. Assessment of FB-I’s Compliance with Articles 5(1)(a), 12 and 13 GDPR	55
F.1 Compliance with Articles 5(1)(a), 12(1), and 13 GDPR	55

F.2 Submissions of FB-I regarding transparency	63
F.3 Analysis and findings of the DPC.....	65
Consideration of first transparency obligation	65
FB-I's submissions in response to the PDD	68
Conclusion and Finding 1	69
Consideration of second transparency obligation	73
FB-I's submissions in response to the PDD	79
Conclusion and Finding 2	82
Consideration of third transparency obligation.....	82
Conclusion and Finding 3	83
Consideration of fourth transparency obligation	83
FB-I's submissions in response to the PDD	85
Conclusion and Finding 4	88
G. Assessment of certain matters concerning Articles 24, 25 and 35 GDPR	89
G.1 Nature, scope, context and purpose of the processing	89
Nature of processing.....	89
Scope of processing	89
Context of processing	90
Purposes of processing	97
G.2 Risks of varying likelihood and severity resulting from the processing	98
Risks described in FB-I's Legitimate Interests Assessments	99
NSPCC Reports concerning Instagram	104
The Berglas Report.....	106
Conclusion.....	117
G.3 Technical and organisational measures, and safeguards implemented by FB-I with regard to processing	117
FB-I's measures and safeguards regarding the processing at issue.....	118
Measures and safeguards concerning the publication of contact information of child users ...	127
Measures and safeguards regarding the public-by-default audience setting	131
Conclusion regarding measures and safeguards	136
H. Assessment of FB-I's Compliance with Article 35 GDPR.....	138
H.1 Compliance with Article 35 GDPR	138
H.2 Submissions of FB-I regarding Article 35 GDPR.....	139
H.3 Analysis and findings of the DPC regarding Article 35	141

Consideration of whether either of the two LIAs prepared by FB-I also complied with Article 35 GDPR	142
Was a DPIA required in respect of the contact information processing?.....	145
Conclusion and Finding 5	149
Was a DPIA required in respect of the public-by-default processing?	150
Conclusion and Finding 6	152
I. Assessment of FB-I's Compliance with Articles 24, 25 and 5(1)(c) GDPR	153
I.1 Compliance with Articles 24, 25, and 5(1)(c) GDPR	153
I.2 Submissions by FB-I regarding Article 25 and 5(1)(c) GDPR	155
I.3 Analysis and findings of the DPC.....	157
FB-I's submission of 9 August 2021	157
Assessment and conclusions regarding FB-I's compliance with Articles 24, 25 and 5(1)(c) in connection with publication of email and/or phone contact information of child users	161
Assessment and conclusions regarding FB-I's compliance with Articles 24, 25 and 5(1)(c) in connection with the public-by-default Instagram processing	168
J. Decision on Corrective Powers	173
K. Order to Bring Processing into Compliance	174
Additional service modifications by FB-I since the PDD	177
Period for compliance	178
Conclusion on Order to Bring Processing into Compliance	179
L. Reprimand	179
M. Administrative Fines	180
M.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;	183
M.1.A The nature of the infringements	187
M.1.B The gravity of the infringements	191
M.1.C The duration of the infringements	195
M.2 Article 83(2)(b): the intentional or negligent character of the infringement;	202
M.3 Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects;.....	210
M.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;...	213
M.5 Article 83(2)(e): any relevant previous infringements by the controller or processor;	214
M.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;	214

M.7 Article 83(2)(g): the categories of personal data affected by the infringement;	216
M.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;	218
M.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;.....	219
M.10 Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and.....	219
M.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.	219
M.12 Decisions on whether to impose administrative fines	221
M.13 Article 83(3)	231
M.13 Articles 83(4) and (5) GDPR	239
N. Summary of Envisaged Action	245

A. Introduction

1. The General Data Protection Regulation¹ (the “**GDPR**”) is a regulation in European Union law on the protection of individuals with regard to the processing of their personal data. The date of application of the GDPR is 25 May 2018.
2. The Data Protection Commission² (the “**DPC**”) was established on 25 May 2018³, pursuant to the Data Protection Act 2018 (the “**2018 Act**”), as Ireland’s supervisory authority within the meaning of, and for the purposes specified in the GDPR.
3. This is a decision (the “**Decision**”) of the DPC pursuant to Section 111 of the 2018 Act, and prepared for the purposes of Article 60 GDPR. I have made this Decision as the decision-maker for the DPC, in the context of an own-volition Inquiry conducted by the DPC pursuant to Section 110 of the 2018 Act (the “**Inquiry**”), concerning the compliance or otherwise of Meta Platforms Ireland Limited, formerly Facebook Ireland Limited (“**FB-I**”),⁴ with its obligations pursuant to Articles 5, 6, 12, 13, 24, 25 and 35 GDPR. The purpose of this Decision is to record the DPC’s views as to whether or not an infringement of the GDPR has occurred and/or is occurring with regard to certain processing of personal data by FB-I. This Decision also sets out the corrective powers that the DPC will exercise, in response to the findings set out below.
4. This Decision further reflects the binding decision that was made by the European Data Protection Board (the “**Board**” or, otherwise, the “**EDPB**”) pursuant to Article 65(2) of the GDPR,⁵ (“the **Article 65 Decision**”) which directed changes to certain of the positions reflected in the draft decision that was presented by the DPC for the purposes of Article 60 (“the **Draft Decision**”), as detailed further below.

B. Background

B.1 The Instagram service

5. Instagram is a global social networking service that allows registered users to communicate with other users through messages, audio, video calls and video chats, and by sending images and video files.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

² Known as “An Coimisiún um Chosaint Sonraí” or, in the English language, the Data Protection Commission

³ Pursuant to the Data Protection Act 2018 (Establishment Day) Order 2018

⁴ Facebook Ireland Limited has changed its name to Meta Platforms Ireland Limited, effective from 5 January 2022, as notified to the DPC by letter from Mason Hayes & Curran, LLP, dated 11 January 2022.

⁵ Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, adopted 28 July 2022

6. Instagram was launched in 2010, and was subsequently acquired by Facebook, Inc. in 2012. On or around 28 October 2021, Facebook, Inc. changed its name to “Meta Platforms, Inc.”. On 28 October 2021, FB-I notified the DPC⁶ that this change only concerned the name of Facebook, Inc., and did not impact the data processing activities or the structures of the organisation.
7. Within the European Union, the Instagram service is provided by FB-I. This Decision considers whether FB-I has complied with its obligations as a controller⁷ under the GDPR.
8. The Instagram service can be accessed using a standalone mobile phone application, but can also be viewed as a webpage using a web-browser. Persons who have not registered as Instagram users can view certain content on the web-browser version of an Instagram user’s profile page. Access to the mobile phone Instagram application is restricted to registered users.
9. Instagram obtains each user’s date of birth as part of account registration. A person must be at least 13 years old to register as an Instagram user. By default, anyone can see a user’s profile and posts on Instagram (referred to as having a “**public account**”). Instagram users can modify their profile settings, so that only users they specifically approve (“**followers**”) can see their profile and posts (referred to as a “**private account**”).
10. The Instagram Service is provided on the basis of a written contract between FB-I and the user, referred to as the “**Terms of Use**”. The version of the Terms of Use which is relevant for the purposes of this Inquiry is that which applied as of 19 April 2018.
11. The collection and use of Instagram users’ personal information is described in the Facebook “**Data Policy**”. The Data Policy refers simultaneously to a number of different services and products owned by FB-I, and is not specific to Instagram. The version of the Facebook Data Policy which is primarily relevant for the purposes of this Inquiry is that which applied as of 19 April 2018. FB-I subsequently revised the Data Policy on 21 August 2020.
12. The Facebook Data Policy contains hyperlinks to websites which contain additional information, including a link to a separate Facebook webpage⁸ which describes FB-I’s legal basis under Article 6 GDPR for processing personal data (the “**Legal Basis Notice**”).
13. In 2016, a new type of Instagram account was introduced, called a “**business account**”. FB-I implemented business accounts on Instagram with the aim of “...allowing more

⁶ Email from the Head of Data Protection of Facebook Ireland Limited to the DPC

⁷ As defined by Article 4(7) GDPR

⁸ https://www.facebook.com/about/privacy/legal_bases

“traditional” businesses the opportunity to better connect their Instagram profile with their “off-Instagram” presence”⁹.

14. Instagram users who switch from a personal account to a business account are shown additional information about their profile and followers (a feature referred to by FB-I as “**Instagram Insights**”), including information on how many times their content was shown to other users, and information on the ages and locations of their profile followers. Prior to September 2019, users who switched to a business account were required to display additional public-facing contact details in the form of an email address and/or a phone number (the “**contact details**”), which were published on the user’s profile page. Personal accounts do not require the publication of email or phone contact information, and do not provide specific fields for the publication of this information.
15. FB-I does not apply age restrictions on the use of Instagram business accounts. Any Instagram user, from the age of 13, may switch from a personal account to a business account.

B.2 Issues referred to Facebook by David Stier

16. Facebook, Inc. (as it was then called) operated a “bug bounty program”¹⁰, which pays financial rewards to security researchers who report security vulnerabilities concerning Instagram. On 22 February 2019, a security researcher named David Stier made a security report to Facebook in the context of the bug bounty program. Mr Stier reported that he had identified a vulnerability in the Instagram platform; in particular, he reported that email addresses and phone numbers of Instagram users were visible in the HTML¹¹ source code of a significant percentage of user profile pages. This issue occurred on the web-browser version of Instagram.
17. For the purpose of his security report, Mr Stier indicated that he had assessed more than 18,000 public Instagram accounts of users who appeared to live in the European Union. Of this sample, Mr Stier estimated that more than 1000 users had visible phone numbers in the HTML source code of their profile pages, and more than 4000 users had visible email addresses in the HTML source code of their profile pages.
18. In his security report, Mr Stier also indicated that email addresses and/or phone numbers of certain users under the age of 18 were visible in the HTML code. Mr Stier provided Facebook with a list of 22 affected users who appeared to be under the age of 18.
19. In subsequent exchanges with Mr Stier, the Facebook security team did not accept that these email addresses and phone numbers had been made public as the result of a bug

⁹ FB-I’s submission to the DPC of 27 October 2020, footnote 16, page 9

¹⁰ Details of the Facebook Bug Bounty Program are available at <https://www.facebook.com/whitehat>

¹¹ Hypertext Markup Language is a standardised system of text annotation used to create webpages

or an error. Facebook indicated that all of the accounts identified by Mr Stier were types of “business account”, and that the publication of email and/or phone information in this context was the result of a choice on the part of those users to switch from personal accounts to business accounts.

20. Notwithstanding its view that no security issue had been identified, the Facebook security team indicated in a response to Mr Stier of 7 March 2019¹² that Facebook would no longer include the phone number or email addresses of users in the HTML source code of profile pages. A representative of the Facebook security team stated:

“After discussing this functionality with the Instagram team we did take steps to remove the contact information from the HTML of the page, since it was not necessary to include in its current form. However this information is still accessible to Instagram users via the Contact button.”

B.3 Issues referred to Supervisory Authorities by David Stier

21. On 17 June 2019, David Stier submitted a breach notification form (the “**Breach Notification**”) to the DPC. In the Breach Notification, Mr Stier stated that between 29 October 2018 and 1 March 2019, Facebook “*leaked the personal contact information of nearly 20%*” of Instagram users by including phone numbers and email addresses in the HTML source code for the web-browser version of Instagram profiles. Mr Stier also stated that users under the age of 18 were affected by this disclosure of information.
22. Mr Stier further reported his concerns to the Hamburg supervisory authority¹³. On 2 July 2019, the Hamburg supervisory authority issued an Article 56 notification to the DPC via the Internal Market Information System in relation to this issue, given the DPC’s position as the probable lead supervisory authority for the processing in question.
23. Mr Stier provided the DPC with correspondence exchanged between him and the Facebook Bug Bounty team, dated between 22 February 2019 and 11 March 2019.

B.4 Introduction of “creator accounts” and modification of Instagram business accounts

24. On 8 July 2019, FB-I introduced a second, alternative type of professional account on Instagram, referred to as a “**creator account**”. Users who switched from a personal account to a creator account were not required to publish their contact information as part of their profile, but could instead decide to display their personal contact information on an optional basis.
25. Further to this, on 4 September 2019, FB-I modified the requirements for switching to a business account, to remove the mandatory requirement to display contact information

¹² Security report of David Stier and response, page 6

¹³ Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

in the form of an email address and/or phone number. FB-I explained the rationale for these service changes as follows¹⁴:

“Over time, it became apparent that more than just “traditional” businesses were utilizing and gaining value from the tools associated with a Business Account (e.g., in-product insights). For example, other users, like professionals and creators – that did not have additional business contact channels -- were utilizing Business Accounts to help grow their presence and build stronger ties with the Instagram community. As discussed in the introduction, Teens have utilized the platform to drive social movements, convert hobbies into in-home businesses, etc., all operating through social media, like Instagram. Some businesses also noted that they preferred to have flexibility in providing additional contact information on their profile and, indeed, preferred to communicate with their audience or customers through direct messaging on Instagram rather than traditional means (like phone or email).

...Therefore, to cater to a larger, diverse base of users of Business Accounts (e.g., creators, entrepreneurs, and businesses of all sizes) Facebook Ireland added the “Creator Account” profile option (on 8 July 2019) and additionally changed the Business Account functionality (on 4 September 2019) so that the display or provision of a business contact option was no longer required.”

26. In August 2020, FB-I reintroduced the practice of publishing email addresses in the HTML source code for business accounts, for the purpose of providing the “email” contact button on the web-browser version of Instagram¹⁵. FB-I suspended this function again in or around November 2020, following additional engagement between David Stier and Facebook.

B.5 Supervisory engagement between the DPC and FB-I

27. On 16 July 2019, a member of DPC staff with the Multinational Technology Supervision Unit contacted FB-I’s Data Protection Officer by email, requesting information on the purported disclosure of personal data, as identified by Mr Stier and described in contemporaneous media articles.

28. In a response of 19 July 2019, a Data Protection Associate on behalf of FB-I stated:

*“...concerning the specific aspect of sharing of phone numbers within the media report, this is related to the Instagram business profile feature, which is an option for people who want to use Instagram for specific purposes. Users are clearly advised that **at least one contact option (phone number or email) must be included for a user to set up a business profile so that the business can be contacted.** The process of enabling business profile features requires a person to explicitly opt-in. When a*

¹⁴ FB-I’s submission to the DPC of 27 October 2020,

¹⁵ FB-I’s submission to the DPC of 18 December 2020, paragraph 55

user opts-in to create a business profile, the user has the option to edit or remove information which they do not want displayed on Instagram. In addition, business profile users always have the ability to change their contact information via account settings.” (emphasis added)

B.6 Preliminary assessment of Mr Stier’s allegations by the DPC

29. To assess the substance of the issues identified by Mr Stier, an Assistant Commissioner with the DPC created a number of Instagram accounts for fictitious child users (aged between 15 and 16) in order to examine the default privacy settings and quality of privacy information provided to child users of Instagram.

30. In the course of conducting the above assessment, the Assistant Commissioner noted that newly registered Instagram accounts are set to “public” by default, unless the user changes their account to “private” after registration is complete. The Assistant Commissioner also noted at this time that child users could switch from a personal account to a business account, and when doing so were required to display either an email address or phone number associated with the business. The Assistant Commissioner also noted the relevance of Recital 38 to the GDPR to the processing in question, which states:

“Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.”

31. On the basis of this preliminary assessment, together with the concerns reported to the DPC by Mr Stier, the DPC Inquiries Committee approved the commencement of an own-volition Inquiry on 19 August 2019. The proposed Inquiry focussed on how the processing at issue complies with the GDPR in respect of child users of Instagram.

32. Additional testing conducted by the DPC in or around September 2019 revealed that FB-I had made changes to the business account switching process. Subsequent to 4 September 2019, users were given an option (which was not previously available) not to display their contact details on their business account profile. In light of this change, the scope of the proposed Inquiry was redrafted to take into account this amendment on the part of FB-I. A redrafted Inquiry proposal was submitted to the DPC Inquiries Committee in July 2020.

33. Having considered the preliminary assessment by DPC staff, the DPC was satisfied on a provisional basis that it was the lead supervisory authority under Article 56(1) GDPR in relation to processing of child users' personal data by FB-I on the Instagram service. Further to this, having considered on a preliminary basis the nature, gravity, and duration of the issues raised, the DPC Inquiries Committee concluded that the commencement of an Inquiry pursuant to section 110(1) of the Act was justified.

C. Commencement and Scope of Inquiry

C.1 Inquiry actions to date

34. Following the decision of the DPC Inquiries Committee, the DPC commenced an own-volition Inquiry pursuant to section 110(1) of the Act, in respect of processing of child users' personal data by FB-I in the context of the Instagram service. The DPC notified FB-I of the commencement of the Inquiry by email of 21 September 2020¹⁶. The notice (the **"Notice of Commencement"**) sent to FB-I outlined the factual background to the Inquiry, the Inquiry procedure, and the issues for determination.
35. The Notice of Commencement included a number of preliminary queries raised by the DPC, to which FB-I provided replies on 27 October 2020.¹⁷
36. Having considered FB-I's replies to the Notice of Commencement, on 27 November 2020, the DPC provided FB-I with a written Statement of Issues¹⁸ (the **"Statement of Issues"**). In the Statement of Issues, the DPC set out the factual summary of relevant issues, and described the matters for determination under the GDPR. FB-I made further submissions to the DPC on 18 December 2020¹⁹, and provided the DPC with an updated Legitimate Interests Assessment on 29 January 2021²⁰.
37. On 11 June 2021, the DPC issued FB-I with a Preliminary Draft of the Draft Decision (the **"PDD"**), and invited FB-I to make submissions on the PDD by 12 July 2021. In correspondence of 24 June 2021, FB-I requested an additional four weeks to respond to the PDD; the DPC acceded to this request. FB-I provided the DPC with its response to the PDD in a submission of 9 August 2021. On 16 August 2021, FB-I furnished the DPC with an additional report, prepared by Mr Austin Berglas of BlueVoyant LLC (the **"Berglas Report"**) in response to certain issues raised in the PDD.
38. The DPC finalised the PDD, taking into account FB-I's submissions dated 9 August 2021 and the Berglas Report. The resulting Draft Decision was circulated to the supervisory authorities concerned (the **"CSAs"**, each one being a **"CSA"**) on 3 December 2021, for

¹⁶ DPC notice of commencement of Inquiry of 21 September 2020

¹⁷ FB-I's submission of 27 October 2020

¹⁸ DPC Statement of Issues letter of 27 November 2020

¹⁹ FB-I's submission of 18 December 2020

²⁰ Titled "Processing minors' data for the provision of the Facebook Products", 28 January 2021

their views, in accordance with Article 60(3) GDPR. Given that the Service entails cross-border processing throughout Europe, all other Supervisory Authorities (the “SAs”, each one being an “SA”) were engaged as CSAs for the purpose of the co-decision-making process outlined in Article 60 of the GDPR. In response, the following CSAs raised objections to the Draft Decision:

- a. The Dutch SA raised an objection on 24 December 2021;
- b. The Hamburg SA (representing the views of the supervisory authorities of Hamburg, Berlin, the Hanseatic City of Bremen and North Rhine-Westphalia on the basis of a coordinated procedure amongst the German SAs) raised an objection on 29 December 2021;
- c. The Norwegian SA raised an objection on 30 December 2021;
- d. The Italian SA raised an objection on 30 December 2021;
- e. The Finnish SA raised an objection on 31 December 2021; and
- f. The French SA raised an objection on 31 December 2021.

39. In addition, the following comments were exchanged:

- a. The Dutch SA exchanged a comment on 24 December 2021;
- b. The Norwegian SA exchanged a comment on 30 December 2021;
- c. The Danish SA exchanged a comment on 30 December 2021; and
- d. The Portuguese SA exchanged a comment on 31 December 2021.

40. Having considered the matters raised, the DPC, by way of a composite response memorandum dated 21 January 2022, set out its responses together with the compromise positions that it proposed to take in response to the various objections and comments. Ultimately, it was not possible to reach consensus with the CSAs on the subject-matter of the objections and, accordingly, the DPC determined that it would not follow them. That being the case, the DPC referred the objections to the Board for determination pursuant to the Article 65(1)(a) dispute resolution mechanism. In advance of doing so, the DPC invited FB-I to exercise its right to be heard on all of the material that the DPC proposed to put before the Board. FB-I exercised its right to be heard by way of its submissions dated 6 April 2022 (the “**Article 65 Submissions**”). The Board adopted its Article 65 Decision on 28 July 2022 and notified it to the DPC and all other CSAs on 3 August 2022. **As per Article 65(1), the Board’s decision is binding upon the DPC. Accordingly, and as required by Article 65(6) of the GDPR, the DPC has now amended its Draft Decision, by way of this Decision, in order to take account of the Board’s determination of the various objections from the CSAs which it deemed to be**

“relevant and reasoned” for the purpose of Article 4(24) of the GDPR. This Decision identifies, below, the amendments to the positions and/or findings proposed in the Draft Decision, that were required to take account of the Board’s Article 65 Decision. For the avoidance of doubt, this Decision does not reference, or engage with, any objections which the Board determined either to be: (i) not “relevant and reasoned”; or (ii) not requiring of any action to be taken on the part of the DPC.

C.2 Temporal scope of Inquiry

41. The temporal scope of this Inquiry includes processing by FB-I during the period between the application of the GDPR on 25 May 2018 and the date of commencement of this Inquiry on 21 September 2020.

C.3 Material scope of Inquiry

42. The Inquiry concerns processing by FB-I of personal data of registered child users of the Instagram service. The 2018 Act provides that the term “child” in the GDPR is to be taken as a reference to a person under the age of 18 years. FB-I provides the Instagram service to persons over the age of 13. As a result, the term “child users” in this Decision should be taken as a reference to registered Instagram users who are aged between 13 and 17 years old. I note that FB-I refers to child users as “teen users” throughout its submissions.
43. In particular, this Inquiry concerns two distinct sets of operations by FB-I in the context of the Instagram service, which each constitute processing of personal data as defined by Article 4(2) GDPR.
44. The first type of processing to be examined concerns the public disclosure of email addresses and/or phone numbers of child users by FB-I (the **“contact information processing”**). In particular, the following processing operations by FB-I are at issue:
 - FB-I permitted child users of Instagram to switch from personal accounts to business accounts;
 - When switching to a business account prior to 4 September 2019, child users were presented with an option screen (titled “Review Your Contact Info”) as part of the switching process. This screen was automatically populated with the user’s information, as obtained by FB-I at the time of user registration. The user could modify the information as populated by FB-I in this form. In order to complete the business account switching process, the user was required to supply either an email address or a phone number. Users who had private Instagram accounts were prompted to switch to a public account as part of the account switching process.

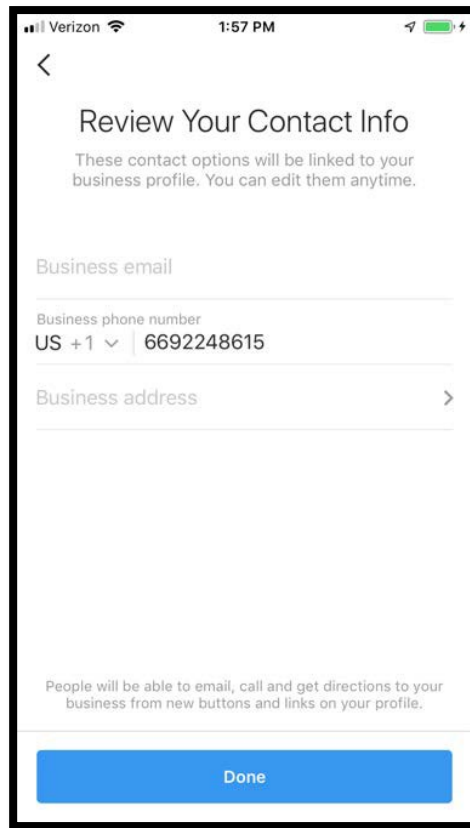


Figure 1 - Pre-September 2019 Option Screen, Appendix J to FB-I's Submission of 27 October 2020

- When switching to a business account subsequent to 4 September 2019, child users were presented with a revised option screen (titled "Review Your Contact Info") as part of the switching process. This screen was automatically populated with the user's information obtained at the time of registration. Users could modify their contact details, or could opt not to provide contact information by pressing the "Don't use my contact info" button at the bottom of the page.

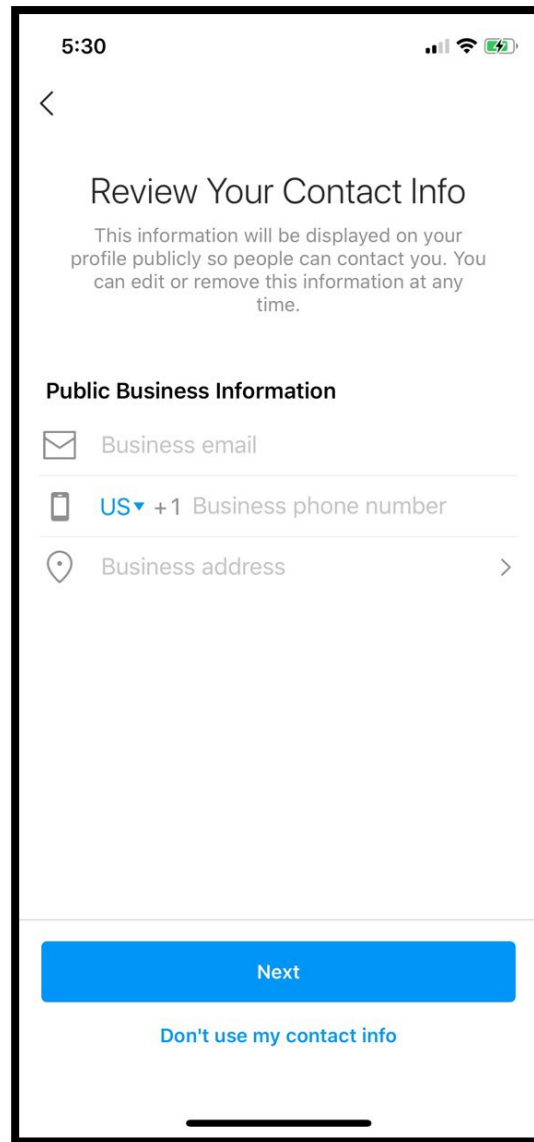


Figure 2 Post-September 2019 Option Screen, Appendix I to FB-I's Submission of 27 October 2020

- Where a child user associated an email address and/or phone number with a business account (whether as a mandatory requirement of switching prior to September 2019, or on an optional basis after September 2019), this phone number and/or email address were published on the user's Instagram profile page, in the form of a "contact button";
- Email addresses and/or phone numbers made public in the context of Instagram business accounts are not encrypted, and are visible as plain text;
- Email addresses and/or phone numbers made public in the context of Instagram business accounts are visible to registered Instagram users on the Instagram mobile application;

- Prior to March 2019, email addresses and/or phone numbers associated with Instagram business accounts were visible (including to persons not registered as Instagram users) as plain text in the HTML source code of the web-browser version of Instagram profile pages; and
 - For a period between August 2020 and November 2020, email addresses associated with Instagram business accounts were visible (including to persons not registered as Instagram users) as plain text in the HTML source code of the web-browser version of Instagram profile pages.
45. The second type of processing which is in scope for the purposes of this Inquiry concerns the default account settings for child users of Instagram (the “**public-by-default processing**”). Instagram profiles can be set to “public” or “private” (referred to by FB-I as the “audience setting” of a profile). Social media content posted to private Instagram accounts can be seen only by Instagram users who are approved by the account holder. Social media content posted to a “public” Instagram account can be viewed by all other Instagram users, and can also be seen to an extent (in the web-browser version) by persons who have not registered as Instagram users.
46. On 16 March 2021, Instagram announced a new process²¹ for when a person under 18 signs up for an Instagram account that gave the user the option to choose between a public or private account. Prior to the introduction of this revised registration process, all users (including child users) were provided with a public account by default, whereby content posted to their account could be seen by all Instagram users (and also seen by persons who had not registered for Instagram, who were accessing the web-browser version of an Instagram account).
47. This Inquiry includes consideration of the “**public-by-default**” setting for personal accounts of child users on Instagram, which applied prior to the revised registration process announced in March 2021. The DPC reserves its position on the extent to which the revised registration process, as announced in 2021, achieves compliance with FB-I’s obligations pursuant to the GDPR.

C.4 Assessment of FB-I’s compliance with the GDPR, and consideration of corrective powers

48. The Statement of Issues sent by the DPC to FB-I on 27 November 2020 set out the matters for determination as part of this Inquiry. These issues concern FB-I’s compliance with the GDPR (and consideration of corrective powers), as follows:

²¹ See further blog post at: <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community>

- Whether the contact information processing by FB-I complied with the conditions set out in Article 6(1) GDPR (i.e. the “legal basis” for processing)²²
- Whether the contact information processing and/or the public-by-default processing complied with FB-I’s obligations under Article 35 GDPR, concerning Data Protection Impact Assessments²³;
- Whether the contact information processing and/or the public-by-default processing complied with FB-I’s obligations under Articles 25(1) and 25(2) GDPR, concerning data protection by design and default²⁴;
- Whether the publication of email addresses and/or phone numbers in the HTML source code of the web-browser version of Instagram profiles of child users was contrary to the principle of data minimisation pursuant to Article 5(1)(c) GDPR;
- Whether FB-I provided child users with information on public-by-default processing, as required pursuant to Articles 5(1)(a), 12(1) and 13 GDPR;
- Whether FB-I provided sufficient information to child users for the purposes of Articles 5(1)(a), 12(1) and 13 GDPR in connection with the contact information processing; and
- Whether the contact information processing and the public-by-default processing complied with FB-I’s obligations under Articles 24(1) GDPR, concerning FB-I’s responsibility to implement appropriate technical and organisational measures (taking into account the risks for the rights and freedoms of child users of Instagram) to ensure and to be able to demonstrate that the processing at issue was and is performed in accordance with the GDPR²⁵;
- In particular with regard to the contact information processing and compliance with Article 24(1) GDPR, whether FB-I implemented appropriate data protection policies as set out in Article 24(2) GDPR²⁶;
- Whether one or more corrective power(s) should be exercised in connection with the findings of the DPC, and if so, which corrective power(s) set out in Article 58(2) should be imposed²⁷.

²² DPC Statement of Issues of 27 November 2020, page 7 and 8

²³ DPC Statement of Issues of 27 November 2020, pages 9 and 10

²⁴ DPC Statement of Issues of 27 November 2020, pages 9 and 10

²⁵ DPC Statement of Issues of 27 November 2020, pages 9, 10 and 11

²⁶ DPC Statement of Issues of 27 November 2020, page 10

²⁷ DPC Statement of Issues of 27 November 2020, page 12

D. Preliminary legal and procedural issues

D.1 Competence of the DPC as lead supervisory authority

49. I have considered whether the processing which is the subject of the Inquiry is cross-border processing under the GDPR, and if so, whether the DPC is competent to act as lead supervisory authority in respect of the processing by FB-I;

50. Cross-border processing is defined in Article 4(23) GDPR as including:

“(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State”.

51. The Facebook Data Policy (which applies to the Instagram service) states²⁸:

“We share information globally, both internally within the Facebook Companies and externally with our partners and with those you connect and share with around the world in accordance with this policy. Information controlled by Facebook Ireland will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes as described in this policy.”

52. This Inquiry pertains to social network activities of child users of Instagram, which can involve the sharing of information with “*millions of followers globally*”²⁹. Based on the information provided by FB-I and information publicly available in the Facebook Data Policy, I am satisfied that the subject matter of the Inquiry relates to cross-border processing of personal data, within the meaning of Article 4(23) GDPR.

53. As the Inquiry relates to cross-border processing of personal data, I have also considered whether the DPC is competent to act as lead supervisory authority in respect of the processing at issue.

54. Article 56(1) GDPR provides that the supervisory authority of the “*main establishment*” of a controller or processor shall be competent to act as “*lead supervisory authority*”

²⁸ Facebook Data Policy of 21 August 2020, section titled “IX. How do we operate and transfer data as part of our global services?”

²⁹ FB-I’s submission of 27 October 2020, paragraph 24

pursuant to Article 60 GDPR. The lead supervisory authority has primary responsibility for supervising the cross-border data processing activity.

55. FB-I is a private company limited by shares having its registered office at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2.
56. In an email of 25 May 2018³⁰ (in correspondence which was independent of this Inquiry) FB-I contacted the DPC to outline the nature of its establishment in Ireland for the purposes of the GDPR. In particular, FB-I stated that “*Facebook Ireland Limited*” was the controller of processing in connection with the Instagram service in the European Union. FB-I further stated that its main establishment for the purposes of the GDPR was in Ireland.
57. In its response to the Notice of Commencement, FB-I also stated that it is the “*controller and service provider of the Instagram service...in the European Region*”³¹.
58. Having considered FB-I’s submissions, the Facebook Data Policy, and the nature of the processing at issue, I am satisfied that FB-I is a controller (within the meaning of Article 4(7) GDPR) with regard to the Instagram processing which is the subject of this Inquiry.
59. I am further satisfied that FB-I has its main establishment in Ireland for the purposes of the GDPR. As such, the DPC was 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 the Complaint, pursuant to Articles 56 and 60 GDPR.

D.2 Procedural issues raised by FB-I prior to the Preliminary Draft Decision

60. By way of letters dated 3 December 2020, 18 December 2018 and 3 February 2021, FB-I raised procedural issues with the DPC regarding the Inquiry procedure. In particular, FB-I queried the reliance of the DPC on a “statement of issues” instead of an “inquiry report” (as in other statutory inquiries relating to FB-I, and as described in the DPC Annual Report for 2018). FB-I also queried the nature and extent of the involvement of the Commissioner for Data Protection in the course of this Inquiry, including the Commissioner’s involvement in the inquiries’ fact-finding elements. FB-I asserted that it was prejudiced as a result of the procedures adopted in this Inquiry, and contended that

³⁰ FB-I’s email of 25 May 2018

³¹ FB-I’s submission of 27 October 2020, page 1. FB-I further stated in its submission of 29 October 2020 in Inquiry IN 20-7-3 that the “*European Region*” at that time included “*Andorra, Austria, The Azores, Belgium, Bulgaria, Canary Islands, the Channel Islands, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, French Guiana, Germany, Greece, Guadeloupe, Hungary, Ireland, Iceland, Italy, Isle of Man, Latvia, Liechtenstein, Lithuania, Luxembourg, Madeira, Malta, Martinique, Mayotte, Monaco, Northern Cyprus, Netherlands, Norway, Poland, Portugal, Réunion, Romania, Saint-Martin, San Marino, Slovakia, Spain, Sweden, Switzerland, UK and UK sovereign bases in Cyprus, Vatican City.*”

the Notice of Commencement gave the impression that the procedural approach adopted in other inquiries would also apply to this Inquiry.

61. In a response of 11 June 2021, the DPC advised FB-I that the DPC is not bound³² to apply identical processes to those set out in the DPC Annual Report for 2018; nor is the DPC required to explain why it has adopted the Inquiry procedure described in the Notice of Commencement (instead of the 2018 procedure).
62. In the DPC letter of 11 June 2021, the DPC noted that the procedure for this Inquiry was described in detail in the Notice of Commencement, and further, the subsequent Statement of Issues identified the core facts as relevant to this Inquiry. The DPC also noted that FB-I responded in detail to the above documents, making lengthy submissions on relevant legal and factual matters. The DPC letter of 11 June 2021 also advised FB-I that it was entitled to “*address any matter of fact or law*” when responding to the Preliminary Draft Decision. Accordingly, the DPC was satisfied that no prejudice arose from the role of the Commissioner for Data Protection, or the procedural steps adopted for the purpose of this Inquiry.

D.3 Purported DPC reliance on draft guidance

63. In its response to the PDD³³, FB-I contended that the GDPR was introduced without guidance regarding child protection measures, as follows:

“From the effective date of the General Data Protection Regulation 2016/679 (“GDPR”), i.e., 25 May 2018, to 2 September 2020 (more than a two-year time span), European regulators issued no specific regulatory guidance interpreting provisions of the GDPR in the youth protection context...”

64. FB-I further states³⁴ that the GDPR “*recognises and endorses the flexibility of controllers to determine compliance measures appropriate for their processing*” and “*provides very little by way of prescriptive requirements*” in relation to the processing personal data of children. FB-I contends that it implemented appropriate measures and safeguards to protect child users of Instagram. FB-I submits that these measures and safeguards were appropriate at the time of application of the GDPR, and have been improved further in the interim.
65. Having made this observation, FB-I contends³⁵ that the DPC has (in the context of this Inquiry) “*implicitly*” applied an interpretation of the GDPR which is taken from a draft

³² Bearing in mind the judgment of Barnville J., delivered on 14 May 2021 in proceedings titled *Facebook Ireland Limited v. Data Protection Commission* 2020 No. 617 JR.

³³ FB-I’s response to the Preliminary Draft Decision, 9 August 2021, paragraph 2

³⁴ Ibid. paragraph 7

³⁵ Ibid. paragraph 11

DPC guidance document on children and the GDPR³⁶, and provides three examples of apparent convergence between the draft guidance and the PDD. FB-I contends that this purported application of draft guidance as the basis for findings in this Inquiry is contrary to the principle of legal certainty. FB-I states that the principle of legal certainty "*dictates that organisations regulated by EU law are entitled to know and understand the specific standards to which they must adhere*"³⁷. By way of comparison, FB-I notes that a statutory code³⁸ implemented in the United Kingdom Information Commissioner was subject to a twelve month transition period.

66. In conclusion, FB-I states³⁹ that it should have been allowed "*an appropriate opportunity to consider this guidance before facing*" the Inquiry, and further states that it has already implemented certain measures to comply with draft guidance and the UK design code.

67. I do not accept FB-I submissions on this issue for the following reasons:

- In its responses, FB-I mischaracterises the nature of GDPR obligations. As a Regulation in EU law, the GDPR is directly effective, and does not require the adoption of national implementing measures for its application. GDPR obligations are established in law without the need for additional guidance, which may be provided by supervisory authorities. Guidance and codes under the GDPR are not binding on controllers, and the application of the GDPR to FB-I as a controller is not contingent on the development of additional context specific rules by supervisory authorities.
- Contrary to FB-I's view that the GDPR endorses *flexibility* on the part of controllers, it is clear that the GDPR emphasises responsibility, accountability and liability⁴⁰ of controllers, as a means of protecting the fundamental rights of data subjects.
- The legislative scheme of the GDPR is risk-based and principles-based. The absence of *prescriptive* obligations regarding children in the GDPR does not imply that supervisory authorities must devise prior guidance before the law will be applicable. It is clear that since the application of the GDPR, each controller must be accountable and responsible for its compliance with the GDPR, taking into account the specific risks and characteristics of processing. There is no legitimate expectation that a controller can await guidance before putting in place appropriate measures and safeguards to protect child users. Further to this, the DPC does not have the power to suspend the application of the GDPR (by means

³⁶ Data Protection Commission – "*Children Front and Centre - Fundamentals for a Child-Oriented Approach to Data Protection*" – Draft version published December 2020

³⁷ FB-I's response to the Preliminary Draft Decision, 9 August 2021 paragraph 10

³⁸ United Kingdom Information Commissioner's Office – "*Age Appropriate Design Code*" – August 2020

³⁹ FB-I's response to the Preliminary Draft Decision, 9 August 2021 paragraph 12

⁴⁰ For example, Articles 5(2) and 24, and Recital 74

of transitional periods) until guidance is finalised, nor would such a suspension be appropriate in circumstances where the GDPR and this Inquiry concern the fundamental rights of children.

- The GDPR entered "*into force*"⁴¹ on 24 May 2016, and has existed in the EU legal order since that date. The GDPR has applied from 25 May 2018. Accordingly, FB-I had a period of two years prior to the application of the GDPR to assess its legal obligations arising from the GDPR.
- FB-I's submission on the need for specific guidance is also contradicted by its simultaneous contention that it has at all times complied with the requirements of the GDPR (even without such guidance), and by the fact that it apparently does not accept the content of the draft guidance in some respects⁴².
- Further to the above, FB-I is incorrect to assert that the DPC has attempted to *implicitly* apply draft guidance as the basis for findings in this Decision. The provisional findings notified to FB-I were based on an assessment of the specific facts that pertain to this Inquiry, and the directly effective obligations of the GDPR. The findings set out in this Decision have not been determined by the content of the draft guidance. The PDD and the draft guidance converge only to the extent that both of these documents apply the underlying principles and obligations of the GDPR, as assessed by the DPC. As can be seen from the detailed assessment that follows in this Decision, the DPC has conducted a case-specific assessment of the law and facts that are relevant to this Inquiry. Accordingly, there has been no direct application (retrospective or otherwise) of the draft guidance in this case, nor was such guidance a necessary prerequisite to the conduct of this Inquiry.

68. On the basis of the above, I do not accept FB-I's submission that it is being held to a standard other than the GDPR. The DPC is satisfied that the GDPR itself created sufficient legal certainty to require FB-I to implement appropriate measures and safeguards, and indeed, FB-I alone was responsible for such measures at the relevant times without the need for additional guidance.

D.4 Legal, factual and procedural issues raised by FB-I concerning the DPC assessment of the purpose of public by default processing

69. This Inquiry involves an assessment of FB-I's compliance with the GDPR, including Articles 5(1)(c), 13(1)(c), 24(1), 25(1), 25(2), and 35(1) GDPR. All of the preceding Articles of the GDPR include explicit references to the *purposes* of processing as a factor which defines the controller's resultant obligations. Accordingly, this Inquiry necessarily involves an

⁴¹ Article 99(1) GDPR

⁴² FB-I submission of 9 August 2021, paragraph 11

assessment of the underlying reasons for processing (i.e. **purpose**) as an inherent element of the GDPR.

70. In its submission of 9 August 2021 responding to PDD, FB-I raised a number of connected issues regarding how the DPC assessed **the purpose** of the public-by-default processing. In particular, FB-I contends as follows:

- that the DPC has erred **in law** by conducting an assessment of the purpose of this processing instead of deferring to the controller's formulation of purpose;
- that the DPC has erred **in fact** by finding that two distinct purposes of processing exist regarding the provision of the Instagram service, depending on whether the user has a public account or a private account; and
- that the DPC introduced novel elements of Inquiry at Preliminary Draft Decision stage, with regard to the DPC's view on the purpose of processing.

71. These three issues are dealt with in this Part of the Decision, as they concern a cross-cutting aspect of my findings and analysis below.

Consideration of FB-I's submissions on the DPC assessment of the purpose of processing

72. In the course of this Decision, the DPC sets out its views on the relevant *purposes* underlying certain types of processing. In its response to the PDD, FB-I contends⁴³ that it is "*incorrect as a matter of law*" for the DPC to "*supplant*" the controller's assessment of purpose with an independent assessment. In particular, FB-I submits that the GDPR "*revolves around*" the Controller's determination of processing, as follows:

*"Supplanting these actual purposes ex post facto with different processing purposes ascribed by the Commission is inconsistent with the GDPR, e.g. because Article 4(7) explicitly states that it is the controller who "determines **the purposes** and means of processing of personal data". It would also result in a lack of legal certainty for controllers as to the nature and extent of their obligations under the GDPR because they would not be able to rely on their own understanding of the processing purposes pursued in order to determine, for example, how to undertake a legal basis assessment or how to provide adequate transparency to data subjects."*

73. Notwithstanding this position, FB-I nevertheless accepts that the DPC is entitled to assess questions of *purpose* in the context of the GDPR, as follows:

"For the avoidance of doubt, Facebook Ireland is not advocating for a position whereby a supervisory authority should never be able to scrutinise the processing purposes identified by controllers. If a supervisory authority has reason to conclude

⁴³ FB-I's submission of 9 August 2021, paragraph 27

that a controller is misrepresenting the processing purpose pursued in a particular context for some reason, then it should of course be able to address that misrepresentation. However, there is no basis for concern in this case that Facebook Ireland is misrepresenting the processing purpose it is pursuing...”

74. I do not accept FB-I’s above submissions, for the following reasons:

- Purpose limitation⁴⁴ is a core principle of the GDPR, which stipulates that personal data must be collected for specified, explicit and legitimate purposes. Further to this, Recital 39 GDPR emphasises that the *“specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data”*.
- Specifically with regard to the assessment of risk under the GDPR, Recital 76 clarifies that any assessment of risk should include an assessment of processing, and risk should be assessed based on objective criteria, in the following manner;
“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”
- The purpose of processing in the context of the GDPR is therefore a key factor which may determine the nature and extent of a controller’s obligations. As such, it is essential to the proper enforcement of the GDPR that supervisory authorities are able to make reasonable and objective assessments of the purpose of processing, taking into account the relevant facts.
- While the definition of a “controller” refers to the person who made decisions about the purposes of processing, FB-I is incorrect as a matter of law to assert that a controller’s stated view on the purpose of processing should consequently be accepted as a matter of fact when assessing other GDPR obligations. The purpose of Article 4(7) GDPR is to define a particular actor in data protection law by reference to actions taken prior to processing. However, nothing in the GDPR creates a presumption that a controller’s stated view on the purpose of processing is correct, or must be accepted automatically by supervisory authorities as a matter of fact. The DPC accepts that a controller may have relevant expertise and knowledge regarding the purpose of processing, which should be taken into account in the assessment of facts. However, the views of a

⁴⁴ Article 5(1)(b) GDPR

controller regarding the purpose of processing cannot supplant an independent assessment by the supervisory authority.

- It is incorrect as a matter of law to suggest that the DPC should only assess the purposes of processing (as a question of fact) if there are reasons to conclude that a controller has otherwise *misrepresented* the purpose of processing. In particular, such an approach would set an artificially high threshold for triggering an assessment by the DPC, i.e. limited only to cases where a controller has intentionally misled the supervisory authority. Such an approach would not account for situations where a controller's assessment of purpose is objectively incorrect, or insufficiently specific for the purpose of the GDPR. Such an approach would also be contrary to the GDPR, insofar that it would place a material restriction on the DPC's tasks and powers⁴⁵ as a supervisory authority, without a proper basis in law.
- Questions of legal certainty do not arise in this context, because a controller is well situated to make a reasonable and objective assessment of the purpose of processing, and can rely on a well-founded assessment of *purpose* as the basis for compliance with GDPR obligations. It is not necessary for a supervisory authority to defer to a controller's particular assessment of purpose, because this question of fact is to be assessed on a reasonable and objective basis. Such an approach (which places the onus on a controller to ensure and demonstrate its compliance with the GDPR) is in conformity with the principle of accountability and the responsibilities of the controller under the GDPR⁴⁶.

75. On the basis of the above, I am of the view that I must be satisfied as to questions of *purpose* where they arise, by making an objective and independent assessment of relevant facts, which is not determined solely by a controller's views on the purpose of processing.

Factual assessment of the purpose of public-by-default processing

76. In addition to its submission that the DPC should defer to the controller's assessment of purpose when assessing compliance with the GDPR, FB-I also contends that the DPC's assessment of the *purpose* of public-by-default processing (as set out in the PDD) is "*factually inaccurate*"⁴⁷ on the basis that the DPC "*...improperly conflates the purpose of processing, a distinct legal concept as determined by the controller, with the practical effect of a default setting*". In particular, FB-I submits⁴⁸ that

⁴⁵ GDPR, Chapter 6

⁴⁶ Articles 5(2) and 24 GDPR

⁴⁷ FB-I's submission of 9 August 2021, paragraph 23

⁴⁸ Ibid. paragraph 25

“...rather than involving a distinct processing purpose, the Account Audience Setting comprises functionality relevant to the provision of the Instagram Service, in that it supports creating, connecting, communicating, discovering, and sharing information. When properly construed, it is a privacy setting like any other – i.e., it operates as a tool that a controller may implement in order to offer users additional control over their personal data when it is being processed as part of a service.”

77. In line with its submissions⁴⁹ in response to the Notice of Commencement and Statement of Issues, FB-I submits that the purpose of processing in connection with the public-by-default processing is as follows⁵⁰:

“The primary processing purpose relevant to the Account Audience Setting is “the provision of the Facebook Products,” which includes the provision of Instagram to all users, including Teens, thereby allowing people to use the platform to share and communicate with a diverse, global community, discover new content, and explore shared interests. Facebook Ireland reasonably reached this position by assessing the context and purpose of the underlying processing at issue, which is the delivery of the Service to its users so they can “create, connect, communicate, discover, and share...on and off Instagram” (as described in the Data Policy and the Terms of Use).”

78. FB-I further contends that the DPC’s assessment of purpose was contradictory, on the basis that the DPC:

“...effectively recognises in the PDD that this is the purpose underlying the processing at issue in the Inquiry when it concluded that Facebook Ireland could avail of Article 6(1)(b) when offering the Business Account feature to Teen Users because such features form “a central part of the [Service]”. As both the Audience Account Setting and the Business Account feature form part of Facebook Ireland’s processing purpose of “providing the Facebook Products”, i.e., the Service, the conclusion in the PDD that the Audience Account Setting involves a distinct and separate processing purpose is inconsistent and contradictory.”

79. On the basis of the above, FB-I contends that the DPC has incorrectly framed the assessment of purpose, and as a consequence, FB-I submits that the DPC has arrived at incorrect conclusions regarding infringements of the GDPR.

80. Article 5(1)(b) and Recital 39 to the GDPR emphasises the need for specified, explicit and legitimate purposes of processing. The Article 29 Working Party⁵¹ (“**WP29**”) published an

⁴⁹ As set out in from paragraph 83 onwards below

⁵⁰ FB-I’s submission of 9 August 2021, paragraph 24

⁵¹ The Working Party was established under Article 29 of Directive 95/46/EC (the Data Protection Directive). It was an independent European advisory body on data protection and privacy. The Working Party has been replaced by the European Data Protection Board under the GDPR.

opinion⁵² on the principle of purpose limitation under EU data protection law. This opinion, (which concerns the equivalent provision to Article 5(1)(b) GDPR under the Data Protection Directive⁵³), addresses the need for specificity of purpose of processing in the following terms⁵⁴:

“Purpose specification lies at the core of the legal framework established for the protection of personal data. In order to determine whether data processing complies with the law, and to establish what data protection safeguards should be applied, it is a necessary precondition to identify the specific purpose(s) for which the collection of personal data is required. Purpose specification thus sets limits on the purposes for which controllers may use the personal data collected, and also helps establish the necessary data protection safeguards.

...The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.

...For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail - usually not meet the criteria of being 'specific'. That said, the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved. In some clear cases, simple language will be sufficient to provide appropriate specification, while in other cases more detail may be required.”

81. Having considered FB-I’s submissions on the purpose of the public-by-default processing, I do not accept the controller’s submissions for the following reasons:

- FB-I is not correct in its view that the Account Audience Setting which was used to switch between public and private accounts is, of itself, the focus of this Inquiry. As is clear from part C2 above, and the below treatment of questions relating to the *purpose* of processing, the material scope of this Inquiry concerns a type of **processing** of personal data on the Instagram platform (i.e. the default publication of social media content to all users of the Instagram service and the world at large), as opposed to an assessment of a user-controller privacy setting.
- The issue of whether the Account Audience Setting is, of itself⁵⁵, a form of processing of personal data is not central to the DPC’s assessment of processing

⁵² Opinion 03/2013 on purpose limitation, WP203

⁵³ Directive 95/46/EC

⁵⁴ WP203 pages 15 and 16

⁵⁵ It is nevertheless possible that FB-I processes personal data in the form of the recorded Audience Account Setting for a given user

in this case, because the DPC has not framed its assessment of public-by-default processing in the manner alleged by FB-I in its submission of 9 August 2021. This Inquiry is primarily concerned with the processing which results from the default setting. In this way, the DPC may assess the Account Audience Setting as an element of the processing, but the Inquiry is not limited to an assessment of the setting.

- By focussing narrowly on the Account Audience Setting (as a technical setting) FB-I fails to acknowledge that this setting has direct consequences in terms of the nature and extent of how FB-I processes personal data. The “*practical effect*” of the Account Audience Setting switches between two different types of processing (social media engagement with known contacts controlled by the user, or engagement with the world-at-large). This Inquiry is concerned with FB-I’s GDPR obligations regarding the default form of processing applied to Instagram user accounts in this regard. The Audience Account Setting is relevant in this context (as a means by which FB-I complies with its wider GDPR obligations) but it is not the sole focus of the Inquiry, as has been clear since the commencement of this Inquiry.
- FB-I submits that all processing which relates to the Audience Account Setting should be construed as a having a single *purpose of processing* – namely “*the provision of the Facebook Products*”. In this way, FB-I contends that public-by-default processing has the same *purpose* as that which applies to private users accounts.
- In the strict sense, FB-I is not incorrect in its view that processing of personal data for both private accounts and public accounts is carried out for the purpose of service provision. However, by reducing the description of purpose to the most basic level of detail, FB-I has not sufficiently specified the purpose of processing as required to comply with the GDPR. In particular, “*service provision*” as a statement of purpose is insufficiently specific; this amounts to an open-ended purpose which could include many different types of processing relating to Instagram.
- By defining the purpose of processing in very general terms, a controller’s compliance with provisions which involve an assessment of the purpose of processing (e.g. Articles 13, 24, 25 and/or 35 GDPR in this case) would lack the required level of transparency, and would fail to take into account the specific reasons for processing which inform subsequent obligations.
- FB-I’s comparison of proposed findings on Article 6(1)(b) in the PDD with my views regarding the purpose of public-by-default processing is based on a misconstruction of the GDPR, and is not accurate. In FB-I’s view, where certain

processing is necessary for the performance of a contract which relates to a service (within the meaning of Article 6(1)(b) GDPR) then the purpose of such processing should be construed simply as “*service provision*”. On this basis, FB-I contends that the DPC has effectively accepted that the purpose of the public-by-default processing is also “*service provision*”, because it has accepted that similar forms of processing may be necessary to perform the Instagram Terms of Use. However, the interpretative approach suggested by FB-I is incorrect, because the assessment of purpose in Article 6(1)(b) is objectively different to the assessment of processing purposes in Articles 13, 24, 25 and 35 GDPR. In particular, it is not correct to conflate contractual purposes as an element of Article 6(1)(b) and processing purposes (which must be assessed in the wider context of the GDPR). The assessment of purpose in Article 6(1)(b) requires the identification of contractual obligations to establish the extent to which processing of personal data may be necessary. Articles 13, 24, 25 and 35 require a processing-specific assessment of purpose in order to contextualise GDPR obligations, and to properly inform the data subject. Although it is not factually incorrect to categorise processing which is necessary to perform the Instagram Terms of Use as being carried out for the purpose of *service provision*, such a broad definition of purpose would be insufficiently specific for the purposes of Articles 13, 24, 25 and 35 of the GDPR, for the reasons described above. Accordingly, I do not accept FB-I’s submission that the proposed findings on legal basis in the PDD were inconsistent with my views on the purpose of public-by-default processing.

82. For the above reasons, I do not agree with the controller’s submissions regarding the DPC’s factual assessment of purpose in this Inquiry, nor do I accept FB-I’s proposed formulation of the purpose of public-by-default processing as being sufficient for the proper application of the GDPR.

Procedural issues regarding the purpose of public-by-default processing

83. In its response of 9 August 2021 to the PDD, FB-I asserts⁵⁶ that the Notice of Commencement of the Inquiry, and subsequent Statement of Issues drafted by the DPC did not include consideration of the *purpose of public-by-default processing* as an issue within the scope of the Inquiry. FB-I contends that the Inquiry to date has “*focused on a single processing purpose -- namely, the display of contact information when Teen Users switched from a personal account to a Business Account*”. FB-I states that the PDD included (purportedly for the first time) consideration of the *purpose* of processing in connection with the public-by-default processing issue.

⁵⁶ Ibid. page 2, footnote 3

84. In this regard, FB-I is incorrect. The Notice of Commencement expressly included⁵⁷ detailed consideration of public-by-default processing from the outset of this Inquiry, as described in Issue 3:

“Issue 3: Whether Facebook is complying with its obligations concerning the potential risks to the rights and freedoms of Child Users arising from its processing of their personal data, including its obligations as a controller under Article 24, its obligations of data protection by design and default under Article 25 of the GDPR, as well as its obligations under Article 35 of the GDPR, in the context of the following issues;

i. The automatic setting of Child Users’ (regular) Instagram profiles to public by default;”

Further to this, Part 3 of the Annex to the Notice of Commencement included as set of queries specifically regarding public-by-default processing, including (for example) questions regarding FB-I’s compliance with Article 25(2) GDPR. Article 25(2) GDPR requires controllers 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” (emphasis added). Accordingly, from the outset of this Inquiry, the DPC has included issues which necessarily include considerations of **the purpose** of public-by-default processing.

85. The clear inclusion of issues regarding purpose in this regard can also be seen in the fact that FB-I made submissions on purpose of this processing in response to the Notice of Commencement, as follows:⁵⁸

“People choose to use Instagram as a platform where they can openly share with a diverse, global community, discover new content, and explore shared interests. Because sharing and maintaining an open exchange with the community of other users is at the heart of Instagram, setting profiles to public per default – including those of Teens – is appropriate and fully in line with user expectations. Users expect to seek, discover, and connect with previously unknown content and communities on Instagram, and the user experience would be hampered for new users – who, by necessity, are still developing connections on Instagram – if their ability to participate would be restricted by default. Default public settings are not only appropriate given the nature of the Instagram Service, which people join in order to use, but also because Facebook Ireland designed Instagram to be safe with Teens specifically in mind. From the moment Teens join Instagram, they enter an environment with

⁵⁷ Notice of Commencement, page 6

⁵⁸ FB-I’s submission of 27 October 2020, pages 16 and 17

strong policies and safeguards in place aimed at providing a safe place to facilitate sharing and expression.”

86. In its response to the Notice of Commencement, FB-I also provided the DPC with a copy of a “Legitimate Interests Assessment”⁵⁹ of 23 October 2020. This document accounts for the purpose of public-by-default processing as follows⁶⁰:

“Due to the nature of the Instagram service and the expectations users have when joining it, all new Instagram accounts are defaulted to public personal accounts, meaning that the account’s audience is not limited to approved followers.”

87. Accordingly, the DPC has been aware of FB-I’s views on the purpose of the public-by-default processing since the early stages of this Inquiry, arising from FB-I’s initial responses to the Notice of Commencement. In particular, FB-I advised the DPC that the purpose of the public-by-default processing was reflective of a purported expectation of new Instagram users that they would “*openly share*” social media content with others.

88. Having considered FB-I’s submission of 27 October 2020, the DPC issued a Statement of Issues letter to FB-I on 27 November 2020. In this letter, the DPC set out in detail the scope of the Inquiry regarding the public-by-default processing, and expressly stated⁶¹ that FB-I’s processing in this regard would be assessed by reference to Articles 13(1), 24(1), 25(1), 25(2) and 35(1) GDPR. In response to the Statement of Issues, FB-I stated⁶² that the DPC should consider the “*purpose of the service*” as a whole when assessing processing in connection with the account audience setting.

89. Taking the above into consideration the DPC is satisfied that FB-I’s submission of 9 August 2021 does not accurately describe the scope and conduct of this Inquiry, for the following reasons:

- With regard to the public-by-default processing, the Notice of Commencement and the Statement of Issues both included consideration of GDPR provisions which expressly involve the *purpose of processing* as a relevant factor. Accordingly, FB-I has no basis to assert that the purpose of processing was included for the first time in the PDD;
- FB-I addressed the purpose of the public-by-default processing in its submissions to the DPC prior to the PDD, and these submissions informed the DPC’s views as set out subsequently in the PDD.

⁵⁹ “Legitimate Interests Assessment (‘LIA’) Processing minors’ data for the provision of the Facebook Products” – Appendix H to FB-I’s submission of 27 October 2020.

⁶⁰ Ibid. page 39

⁶¹ Statement of Issues letter, pages 8 to 11

⁶² FB-I’s submission of 18 December 2020, paragraphs 20-22

90. In its submission of 9 August 2021, FB-I also contends that the DPC ought to have notified the controller of its views on the purpose of public-by-default processing at an earlier stage of the Inquiry⁶³, as follows:

“...to-date in this Inquiry the Commission has not asked Facebook Ireland to explain the underlying processing purpose in connection with the Account Audience Setting. Instead, the Commission introduced a new processing purpose – namely, “public-by-default processing” – formulated and defined by the Commission for the first time in the PDD.”

91. FB-I contends that the DPC’s approach to *purpose* in this regard has caused prejudice, in the following terms⁶⁴:

“In introducing this new processing purpose for the first time in the PDD, the Commission has impeded Facebook Ireland’s right to be heard because Facebook Ireland is only able to address this point at this late stage in the Inquiry process and in the context of an already made preliminary finding paired with detailed preliminary corrective measures. The previous stages of this inquiry involved the Commission gathering information and then identifying key issues and explaining its positions on these. We respectfully suggest that it was during those stages that the Commission should have engaged with Facebook Ireland on this important issue underpinning various findings and corrective measures.

92. The DPC’s view on this purpose of processing is not a “new” legal and factual issue. The purpose of the PDD is to inform the controller as to the position of the DPC regarding the detailed application of the law to the facts of the Inquiry, and to obtain the controller’s response. It is appropriate that the DPC’s detailed views on the application of the law to the facts should first be informed by the controller’s submissions. The preliminary views set out in the PDD were the result of a detailed assessment of two sets⁶⁵ of submissions from the controller. The DPC’s view on the *purpose of public-by-default processing*, as set out in the PDD, represents a detailed application of the law to the facts, as provided to the DPC by FB-I in its earlier submissions. In particular, this view of the DPC was developed having first considered the controller’s view on purpose (as described in its earlier submissions). The DPC does not accept that it would have been appropriate to provide its views at an earlier point in the Inquiry. Such an approach would be premature when the controller had not yet provided its legal and/or factual submissions to the DPC. Further to this, the controller has been allowed an unrestricted opportunity to respond to the DPC’s views as contained in the PDD, and has provided detailed submissions in this regard.

⁶³ FB-I’s submission of 9 August 2021, paragraph 5, page 4

⁶⁴ FB-I’s cover letter to its submission of 9 August 2021, page 2

⁶⁵ i.e. the responses to the Notice of Commencement and Statement of Issues

93. Having considered the Notice of Commencement, the Statement of Issues, and FB-I's submissions, I am satisfied that the controller was on notice since the commencement of this Inquiry that this aspect of *purpose* was in scope, and indeed, FB-I made specific submissions concerning the purpose of this processing, prior to the PDD. The DPC is therefore satisfied that no prejudice arises, because the controller has engaged with the DPC on questions of *purpose* from the earliest stages of this Inquiry. The DPC is further satisfied that no prejudice arises because FB-I's response to the PDD has been considered by the DPC in full when finalising this Decision, including certain matters which FB-I could have raised at an earlier point in the Inquiry process, but did not mention until after the first two rounds of submissions (e.g. certain mitigating actions first described by FB-I in its response to the PDD and which are considered at paragraphs 328 to 336 below).

Preliminary conclusion on the purpose of public-by-default processing

94. On the basis of the matters addressed in Part D.4 of this Decision, the DPC is satisfied that:

- the DPC has not erred in law by conducting an independent assessment of *purpose* as an aspect of GDPR compliance. FB-I is not correct in its contention that deference is due to a controller under the GDPR in the assessment of the purpose of processing; and
- the DPC has not erred in fact by making a specific assessment of processing with regard to the purpose of public-by-default processing. Further to this, very general statements of processing (e.g. "*service provision*" as a purpose of processing) are too vague to meet the requirements of the GDPR; and
- it has been clear since the outset of this Inquiry that the DPC would assess questions regarding the *purpose of public-by-default processing*. It was appropriate and necessary for the DPC to set out its provisional views on this *purpose* as part of the PDD, and not at an earlier stage, because it would be premature for the DPC to form a detailed view on the application of the law to the facts until the controller provided sufficient information to the DPC (i.e. the information contained in FB-I's responses to the Notice of Commencement and Statement of Issues). Having formed a preliminary view on the *purpose* of this processing, the DPC notified FB-I of this position, and allowed FB-I to respond to any legal or factual issues arising. The DPC therefore does not accept that FB-I's position has been prejudiced by the procedure adopted by the DPC.

95. Accordingly, I do not accept FB-I's legal, factual and procedural contentions as set out in its response of 9 August 2021, in connection with the DPC assessment of the *purpose of public-by-default processing*. As a result, where such issues arise in the remainder of this Decision (in the context of FB-I's compliance with specific GDPR provisions) I have

conducted the necessary legal and factual assessment of the purpose of processing, as an essential component of GDPR compliance, taking into account the extensive submissions of the controller on this issue.

D.6 Assessment of “risk” in the context of the GDPR

96. In its response and cover letter of 9 August 2021, FB-I contends that the DPC has not correctly assessed questions of risk as they arise in relation to the scope of this Inquiry. In particular, FB-I states⁶⁶:

“A number of the conclusions reached in the PDD appear to be based on assumptions (e.g., about hypothetical off-platform risks stemming from the two issues that are the subject of the Inquiry, as explained in the PDD). In particular, the Commission has expressed views in the PDD about the potential risks for Teen Users (as defined in the Response to the PDD), as identified by Facebook Ireland in the scope of its legitimate interests assessment. However, the Commission’s views, as expressed in the PDD, fail to consider the safeguards Facebook Ireland in fact provides to address and mitigate against these potential risks, including the measures in place to mitigate the risk of potential off-platform harm (e.g., around child protection issues and/or scraping). In addition, it appears from the PDD that the Commission has failed to investigate the potential risks outlined in the PDD and has failed to identify evidence to substantiate the conclusions it has reached in relation to those potential risks. The fact that the Commission’s positions are based on supposition and/or speculation as to the perceived potential risks for Teen Users, inhibits Facebook Ireland’s ability to respond to the preliminary findings made against it in the PDD.”

97. Having considered FB-I’s assessment of risk as set out in the earlier Inquiry stages of this Inquiry, and the additional factual matters set out in FB-I’s submissions of 9 August 2021 (including the subsequent Berglas Report procured by FB-I), I am satisfied, for reasons that are stated further in this Decision, that the DPC has conducted an appropriate assessment of risk for the purposes of this Inquiry. While I have considered all submissions made by FB-I in the course of this inquiry, including its responses to the PDD, I am satisfied that the factual matters which FB-I raised following the PDD could equally have been brought to the attention of the DPC in response to the Notice of Commencement and/or Statement of Issues; FB-I was on notice of the relevant issues from the earliest stages of the inquiry. Notwithstanding the fact the FB-I has expanded its factual submissions in response to the PDD, I am satisfied that the treatment of risk and associated factual matters in this Decision constitutes a comprehensive treatment of the factual aspects of this Inquiry, informed by multiple rounds of submissions from FB-I, and other relevant sources of information notified to the controller.

⁶⁶ FB-I’s cover letter to its response of 9 August 2021, page 2

D.7 Purported failure on the part of the DPC to provide a “Statement of Facts”

98. In its cover letter to its response of 9 August 2021, FB-I submitted that certain procedural steps had been omitted, as follows:

“The Commission has departed in a number of significant respects from the process it indicated it would adopt in this inquiry in the [Notice of Commencement]. We refer you in this regard to prior correspondence in respect of the failure by the Commission to issue a Statement of Facts. While we are grateful for the Commission’s response when these concerns were raised previously, the practical consequences of this, and the very real prejudice this has caused to Facebook Ireland, has now become apparent.”

FB-I further contends that the purported omission of a Statement of Facts has prejudiced the controller’s procedural rights *“because Facebook Ireland is only able to address this point at this late stage in the Inquiry process and in the context of an already made preliminary finding paired with detailed preliminary corrective measures”*.

99. The Notice of Commencement stated⁶⁷ that the DPC may issue FB-I with:

“...a statement of facts as established up to that point together with a summary of the issues arising in the Inquiry which the DPC considers will fall for decision...”

The DPC subsequently issued a Statement of Issues to FB-I, which contained both *“Facts relied on by the DPC”* as well as descriptions of matters which were *“For Determination by the DPC”*. It therefore appears that, notwithstanding a minor difference in terminology (i.e. the use of the title “Statement of Issues” instead of “Statement of Facts”), the Statement of Issues provided to FB-I exactly meets the description of this Inquiry stage as set out in the Notice of Commencement. On this basis, I do not accept FB-I’s submission that it was not provided with a statement of facts.

100. I do not accept FB-I’s submission that an additional Statement of Facts ought to have been produced prior to the PDD, or that FB-I ought to have been provided with the DPC’s concrete preliminary views on the application of the law to the facts, before preparation of the PDD. The Preliminary Draft Decision stage of the Inquiry informs the controller of the DPC’s provisional views on possible infringements of the GDPR, and includes more detailed legal and factual assessment, informed by the controller’s submissions. In this context, and prior to making its response to the PDD, FB-I was advised⁶⁸ as follows:

⁶⁷ Notice of Commencement, paragraph 20

⁶⁸ DPC letter to FB-I of 11 June 2021

“While [FB-I’s response to the PDD] has been be invited by reference to the contents of the [PDD], it will, in principle, be open to your client to address any matter of fact or law which it considers to bear on the issues under examination.”

In response to the PDD, FB-I made a 78 page submission that addressed the legal, factual and procedural aspects of this Inquiry. This submission supplements and expands on the already extensive responses of FB-I provided prior to the PDD. The content of this submission has been considered by the DPC in producing this Decision.

101. In circumstances where FB-I has provided extensive legal and factual submissions in response to the DPC’s provisional findings in the PDD, I am satisfied that the controller has been provided with an opportunity to be heard in relation to this Inquiry.

E. Consideration of Article 6 GDPR

Compliance with Article 6(1) GDPR

102. Following the issues for determination set out in the Statement of Issues, this Inquiry considers whether the processing of contact information by FB-I was contrary to Article 6(1) GDPR.

103. Article 6(1) GDPR stipulates that the processing of personal data is lawful only if one of the conditions set out in Article 6(1)(a) to (f) is met. Compliance with Article 6(1) is referred to as having a “*legal basis*” for processing. Having a legal basis under Article 6(1) GDPR is necessary but not sufficient for processing to be lawful; controllers must also meet the broader obligations set out in the GDPR. Article 6(1)(b) provides that one such legal basis is where processing is necessary for the **performance of a contract** to which the data subject is party.

104. Article 6(1)(f) also provides a legal basis for processing where the following three conditions coincide:

- first, the pursuit of a **legitimate interest** by the data controller or by a third party;
- second, the need to process personal data for the purposes of the legitimate interests pursued;
- and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.

Submissions of FB-I regarding Article 6 GDPR

105. In submissions to the DPC, FB-I indicated that it relied separately on Articles 6(1)(b) and 6(1)(f) GDPR for the contact information processing in respect of child users.

106. In describing the applicable legal bases for the contract information processing, FB-I states⁶⁹:

“[o]ffering Instagram Business Accounts -- and the display of a contact option in connection with an Instagram Business Account -- is an integral part of the service Instagram offers to all users...Moreover [child users] have proven that they are (at least) equally capable of formulating creative businesses or initiatives on Instagram that can rely on the tools available to Business Accounts, and Facebook Ireland sees no reason why they should be deprived of the opportunity to grow such businesses or initiatives on a platform that is built to be safe for everyone.”

In that context, and depending on the user in question, Facebook Ireland relies on two primary legal bases for the purposes of providing...the Facebook products (including Instagram), which includes provision of the Instagram Business Account and the display of a contact option in connection with an Instagram Business Account.”

107. FB-I submits⁷⁰ that Article 6(1)(b) GDPR is the “most appropriate” legal basis for the contact information processing, because this processing is “central” to the Instagram service as provided to business account users. Notwithstanding this, FB-I states that Article 6(1)(f) GDPR also provides an appropriate legal basis for “users who cannot validly enter into enforceable contracts (or have limited capacity to do so) under their Member State’s laws”⁷¹.

108. FB-I further outlines⁷² the criteria which determine the applicable legal basis relied on by FB-I for processing, as follows:

“There is no harmonisation of contract law across the EU, and Member States follow different models as to the enforceability of agreements concluded by people between 13 and the age of majority. However, in a number of Member States (e.g. Spain and the Netherlands) Teen Users are able to enter legally enforceable contracts before they are 18.”

109. The Instagram Terms of Use which applied⁷³ during the temporal scope of the Inquiry stated:

*“If you are a consumer and habitually reside in a Member State of the European Union, **the laws of that Member State will apply** to any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms (“claim”), and*

⁶⁹ FB-I’s submission of 27 October 2020, paragraphs 16 and 17

⁷⁰ FB-I’s submission of 27 October 2020, paragraph 18

⁷¹ FB-I’s submission of 27 October 2020, paragraph 18

⁷² FB-I’s submission of 29 October 2020 in Inquiry IN 20-7-3, footnote 38

⁷³ Instagram Terms of Use of 19 April 2018, section titled “How We Will Handle Disputes”

you may resolve your claim in any competent court in that Member State that has jurisdiction over the claim.” (emphasis added)

110. It is therefore FB-I’s position that one of two legal bases under Article 6(1) applied to the contact information processing, varying from country to country and depending on the applicable national law provisions governing the contractual capacity of children. Where a child user resided in an EU Member State which allowed persons under 18 years to enter into legally enforceable contracts, FB-I relied on Article 6(1)(b) as the legal basis for processing. Where national law provisions did not allow the child user to enter into a legally enforceable contract with FB-I, the controller relied on Article 6(1)(f) as the basis for processing.

111. With regard to the three elements of Article 6(1)(f) GDPR, FB-I submitted that the display of contact information of users was in pursuit of FB-I’s legitimate interest of creating products and features that allow child users to communicate with others and to engage with information which is relevant to their interests⁷⁴. FB-I also submitted that the processing was in pursuit of the legitimate interests of other Instagram users who wished to communicate directly with the holder of a business account⁷⁵.

112. FB-I contends⁷⁶ that the contact information processing was necessary for the pursuit of the above interests, in order to allow for “*meaningful engagement*” between child users who operated business accounts, and other users who wished to communicate with the child user. In this context, FB-I stated that child users who operate business accounts are “*a foundation of the diverse Instagram community and equally have an interest to build up their brands, fortify connections with their followers, and deliver engaging content in the best way possible*”.

113. FB-I submits⁷⁷ that the processing was “*reasonable, proportionate, and within the reasonable expectations of Teen Users*”. In particular, FB-I contends that the business account switching process sufficiently clarified the processing entailed.

114. With regard to the balancing of the interests and fundamental rights and freedoms of the data subject against the legitimate interests in question, FB-I submits⁷⁸ that

- it provided sufficient information to explain the contact information processing and the public nature of the processing, including specific information for child users and parents;
- the publication of contact information was made optional after September 2019;

⁷⁴ FB-I’s submission of 27 October 2020, paragraph 21

⁷⁵ FB-I’s submission of 27 October 2020, paragraph 22

⁷⁶ FB-I’s submission of 27 October 2020, paragraphs 23 and 24

⁷⁷ FB-I’s submission of 27 October 2020, paragraphs 25 to 29

⁷⁸ FB-I’s submission of 27 October 2020, paragraphs 30 to 37

- FB-I excluded child users from its initiatives to promote business accounts;
- FB-I implemented security and safety measures in connection with the Instagram platform;
- FB-I implemented “*content policies, reviewing processes, proactive detection, and product interventions*” in respect of the Instagram platform;
- by allowing child users to switch to a business account, FB-I supported child users’ “*fundamental rights to conduct a business, express themselves, communicate, and engage with information relevant to their interests and passions, while building community and their own businesses, brands, or initiatives*”; and
- by allowing child users to switch to business accounts without additional approval mechanisms, FB-I complied with the principle of data minimisation and prevented unnecessary barriers to the use of business accounts.

115. On the basis of the above submissions, FB-I concluded that the legitimate interests in question were not overridden by the interests or fundamental rights and freedoms of child users. FB-I therefore submitted that the contact information processing was lawful under Article 6(1)(f) GDPR (with regard to child users who did not have capacity to enter into a contract with FB-I).

Analysis and findings of the DPC

Assessment of processing on the basis of Article 6(1)(b) GDPR

116. On registering for a personal Instagram account, a data subject agreed to the Instagram Terms of Use. I note FB-I’s submission that it relies on Article 6(1)(b) GDPR only to the extent that a child user has capacity to enter into an enforceable contract. Section 1 of the Instagram Terms of Use (titled the “*The Instagram Service*”) listed nine service areas. Section 1 of the Terms of Use stated:

“...[t]he [Instagram] Service is made up of the following aspects (the Service):

Offering personalized opportunities to create, connect, communicate, discover, and share. People are different. We want to strengthen your relationships through shared experiences you actually care about. So we build systems that try to understand who and what you and others care about, and use that information to help you create, find, join, and share in experiences that matter to you. Part of that is highlighting content, features, offers, and accounts you might be interested in, and offering ways for you to experience Instagram, based on things you and others do on and off Instagram.”

117. I note that the Terms of Use do not make specific reference to the operation of business accounts on Instagram, nor do they reference the publication of contact information. However, in the Draft Decision, I expressed the view that Article 6(1)(b) GDPR does not require the inclusion of express contractual provisions pertaining to processing in order to provide a legal basis. It is sufficient for the purpose of Article 6(1)(b) that processing of personal data is necessary for the performance of a contract with the data subject. I further note FB-I's submissions that business accounts are a central part of the Instagram service. In considering the above section of the Terms of Use, I proposed a finding of compliance with Article 6(1)(b) GDPR in the Draft Decision on the basis that I was satisfied that the performance of the contract can be regarded as including processing associated with the business account feature, on the basis that this social media tool allows users to *"create, find, join, and share in experiences"* with other people (as described in the Terms of Use), and forms a central part of the Instagram service as offered. I was also satisfied that the publication of contact information in the context of business accounts may be regarded as necessary processing for the purpose of Article 6(1)(b) GDPR (subject to my adverse findings below which address to FB-I's wider GDPR obligations in relation to the contact information processing).

118. Based on the Terms of Use, I am satisfied that the contact information processing could be necessary for the performance of FB-I's Terms of Service with its users. Accordingly, and for the purpose of section 111(1) of the 2018 Act, and on the facts of this Inquiry as they are currently known to me, I am not satisfied that an infringement by FB-I occurred to the extent that it relied on Article 6(1)(b) GDPR as a legal basis for processing personal data of certain child users.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

119. The supervisory authorities of Germany (via Hamburg), Finland, France, Italy, the Netherlands and Norway each raised an objection to the finding proposed under this particular heading. The objections identified various concerns in relation to the necessity of the processing for the performance of the contract under examination.

120. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, these matters were included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution process. Having considered the merits of the objections, the Board determined as follows:

" ...

80. The EDPB recalls that personal data can be processed on the basis of Article 6(1)(b) GDPR when: (1) the processing takes place in the context of the performance of a contract with the data subject and (2) that processing is

necessary for the performance of that particular contract with the data subject⁷⁹.

81. With respect to the existence of a contract, the EDPB takes note of the objections raised by the DE SAs⁸⁰ and FI SA⁸¹, as well as the IT SA⁸² and FR SA⁸³, which questioned the failure by the IE SA to assess and conclude on the existence of a valid contract between Meta IE and the child users insofar as it concerns the contact information processing. The NL SA argued that, first, the LSA did not assess adequately in the Draft Decision if a contract was in place between Meta IE and the data subjects for the provision of the Instagram business account and, second, the NL SA raised doubts about the validity of such contract⁸⁴.

82. In the Draft Decision, the IE SA found that, when registering for a personal Instagram account, a data subject agreed to the Instagram Terms of Use⁸⁵. The IE SA further found, in the light of Meta IE's submissions, that the performance of a contract legal basis could be invoked by Meta IE in relation to processing associated with the business account feature on the basis of the Terms of Use⁸⁶.

83. In its submissions, Meta IE argued that SAs do not have competence to assess validity of contracts⁸⁷ and anyway the Draft Decision clearly referred to a contractual relationship between Meta IE and each user based on the Terms of Use⁸⁸. Meta IE also claimed that it had no legal obligation under the GDPR to include a specific reference to Business Accounts in the Instagram Terms of Use and thus the lack of such reference has no impact on the assessment of whether the processing is necessary for the performance of a contract⁸⁹ and is not contrary to Article 12 GDPR⁹⁰.

84. As recalled above, one of the prerequisites for a controller to be able to rely on Article 6(1)(b) GDPR as a legal basis for the processing of personal data is that the processing takes place in the context of the performance of a contract. As previously stated by the EDPB, this condition more specifically implies that a controller, in line with its accountability obligations under Article 5(2) GDPR, has to be able to demonstrate that (a) a contract exists and (b) the contract is valid pursuant to applicable national contract laws⁹¹.

85. In order to assess whether Meta IE could have relied on Article 6(1)(b) GDPR for the contact information processing, the EDPB analyses in the following paragraphs

⁷⁹ Footnote from the Article 65 Decision: Art. 6(1)(b) GDPR.

⁸⁰ Footnote from the Article 65 Decision: DE SAs objection, p. 3-4.

⁸¹ Footnote from the Article 65 Decision: FI SA objection, paras. 4-5.

⁸² Footnote from the Article 65 Decision: IT SA objection, p. 1.

⁸³ Footnote from the Article 65 Decision: FR SA objection, paragraph 11.

⁸⁴ Footnote from the Article 65 Decision: NL SA objection, paragraphs 9-11.

⁸⁵ Footnote from the Article 65 Decision: Draft Decision, paragraph 114.

⁸⁶ Footnote from the Article 65 Decision: Draft Decision, paragraph 115.

⁸⁷ Footnote from the Article 65 Decision: IE Article 65 Submissions, paragraphs 50-51.

⁸⁸ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 52.

⁸⁹ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraphs 53-54.

⁹⁰ Footnote from the Article 65 Decision: Meta IE Article 65 submissions, paragraph 55.

⁹¹ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 26.

whether the processing at stake is **necessary** for the performance of the alleged contract with the data subjects in the case at hand.

86. In its submissions, Meta IE claimed that insofar as “necessity” is concerned, the CSAs ignored the relevant facts and considerations during the period when Business Accounts were first offered and erred in: (1) applying an overly strict view of the element of necessity for the purposes of Article 6(1)(b) GDPR, and (2) improperly seeking to retroactively find a violation of Article 6(1)(b) GDPR by virtue of a subsequent product modification, which has dangerous implications for controllers seeking to develop and evolve their products over time in respect of user privacy and safety⁹². According to Meta IE, “the Business Account was created for Instagram in 2016 and, as relevant for the time, it was built around the notion of a “traditional” business, which may have used Instagram to support its external (i.e., off-Instagram) presence, like a website or brick-and-mortar establishment. To enable the off-Instagram promotion of and contact with the business, the Business Account functionality included a “Contact” button to allow the Instagram community to communicate with the business through a contact channel outside of Instagram (e.g., a business phone or email)” and “the EDPB must assess the element of necessity under the correct conceptual framework having regard to the specific purpose of the processing at issue at the time, in line with its prior guidance”⁹³. In addition, according to Meta IE, compliance with Articles 5(1)(c) and 6(1)(b) GDPR must be considered separately, the LSA’s finding on Article 5(1)(c) GDPR was narrow in scope, and, moreover, Articles 5(1)(c) and 6(1)(b) GDPR have distinct and separate meanings, thus a finding of non-compliance with Article 5(1)(c) GDPR does not and cannot equate automatically to a finding of non-compliance with Article 6(1)(b) GDPR⁹⁴.

87. The EDPB recalls that the concept of necessity has an independent meaning in Union law, which must reflect the objectives of data protection law⁹⁵. In particular, as the CJEU has stated: “[a]s regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary”⁹⁶.

88. When analysing the performance of a contract legal basis, the necessity requirement has to be interpreted strictly. As stated earlier by the Working Party 29 (hereinafter

⁹² Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 58.

⁹³ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 61.

⁹⁴ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraphs 67-72.

⁹⁵ Footnote from the Article 65 Decision: *Heinz Huber v Bundesrepublik Deutschland* (Case C-524/06, judgement delivered on 18 December 2008, ECLI:EU:C:2008:724) (hereinafter, “**C-524/06 Huber**”), paragraph 52.

⁹⁶ Footnote from the Article 65 Decision: *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiksme’* (Case C-13/16, judgement delivered on 4 May 2017, ECLI:EU:C:2017:336) (hereinafter, “**C-13/16 Rīgas**”), paragraph 30.

“WP29”⁹⁷, this “provision must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller”⁹⁸.

89. The EDPB recalls that for the assessment of necessity under Article 6(1)(b) GDPR, “[i]t is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance”⁹⁹. As the EDPB has previously stated, regard should be given to the particular aim, purpose, or objective of the service and, for applicability of Article 6(1)(b) GDPR, it is required that the processing is objectively necessary for a purpose and integral to the delivery of that contractual service to the data subject¹⁰⁰.

90. Moreover, the EDPB notes that the controller should be able to justify the necessity of its processing by reference to the fundamental and mutually understood contractual purpose. This depends not only on the controller’s perspective, but also on a reasonable data subject’s perspective when entering into the contract¹⁰¹. In this context, the EDPB recalls that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data¹⁰².

91. Regarding the objective and purpose of the specific contract, Meta IE claimed that, when the Business Account was created, it was built around the notion of a “traditional” business and was aimed to allow the Instagram community to communicate with the business through a contact channel outside of Instagram¹⁰³. The IE SA found that “the business account feature, on the basis that this social media tool allows users to ‘create, find, join, and share in experiences’ with other people (as described in the Terms of Use), and forms a central part of the Instagram service as offered”¹⁰⁴.

92. While the EDPB agrees that processing may be objectively necessary for the

⁹⁷ Footnote from the Article 65 Decision: The Working Party 29 - a predecessor of the EDPB - was established under Article 29 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, “**Directive 95/46/EC**”) and had a role, inter alia, to contribute to uniform application of national measures adopted under the Directive. Many of substantive principles and provisions of the GDPR already existed in the Directive 95/46/EC, thus WP29 guidance in this respect is relevant for the interpretation of the GDPR.

⁹⁸ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, adopted on 9 April 2014 (hereinafter, “**WP29 Opinion 06/2014 on the notion of legitimate interests**”), p. 16.

⁹⁹ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 17.

¹⁰⁰ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 30.

¹⁰¹ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 32.

¹⁰² Footnote from the Article 65 Decision: Recital 38, GDPR: “Such specific protection should, in particular, apply to [...] the collection of personal data with regard to children when using services offered directly to a child”.

¹⁰³ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 61.

¹⁰⁴ Footnote from the Article 65 Decision: Draft Decision, paragraph 115.

performance of a contract even if not specifically mentioned in the contract¹⁰⁵, it should be possible for an ordinary user to identify the “fundamental and mutually understood” contractual purpose based on the information presented by the controller¹⁰⁶.

93. Considering the high-level information provided to child users regarding the Instagram service in the Terms of Use¹⁰⁷ and that no specific information about the Business Account feature was provided to the child users¹⁰⁸, the EDPB considers that the publication of the contact details on their profiles could have not been reasonably expected by such child users in the context of their use of Instagram, including the business account feature. Further, the EDPB does not agree that the contact information processing, in respect of the child users, could be considered as “integral” or “central” to the Instagram service, including the business account feature. Moreover, as correctly noted by the IE SA, it is possible to operate a professional profile without also publishing contact information¹⁰⁹.

94. Furthermore, the EDPB recalls that the assessment of what is necessary involves a combined, fact- based assessment of the processing for the objective pursued. If there are realistic, less intrusive alternatives, the processing is not necessary¹¹⁰. In this respect, the principle of proportionality should also be taken into account¹¹¹.

95. The EDPB observes that, if the publication of the contact details was indeed intended for traditional businesses only as Meta IE claims, it was technically possible to distinguish them from the child users during the registration process based on age information¹¹². It would have therefore been possible to avoid publishing child users’ contact information, even while maintaining the contact button option for “traditional” businesses.

96. The EDPB further considers that in the present case the analysis of necessity should be supported by the above-mentioned analysis of the existence of less intrusive means. However, the IE SA did not analyse in the Draft Decision whether other less intrusive means were available to effectively achieve the objective pursued. In this regard, the existing possibility to contact users directly through direct messaging within the platform should have been taken into consideration. In fact, it is clear from the Draft Decision that Meta IE was aware that certain business account users preferred to communicate with their audience through direct messaging on

¹⁰⁵ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 27.

¹⁰⁶ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 33.

¹⁰⁷ Footnote from the Article 65 Decision: As identified by the IE SA, the relevant aspect of the service (Section 1, Instagram Terms of Use, version of 19 April 2018) was presented as follows: “*personalized opportunities to create, connect, communicate, discover, and share*”, see Draft Decision, paragraph 114.

¹⁰⁸ Footnote from the Article 65 Decision: Draft Decision, paragraph 115.

¹⁰⁹ Footnote from the Article 65 Decision: Draft Decision, paragraph 353.

¹¹⁰ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 25.

¹¹¹ Footnote from the Article 65 Decision: *Volker und Markus Schecke and Eifert* (Cases C-92/09 and C-93/09, judgement delivered on 9 November 2010, EU:C:2010:662) (hereinafter, “**C-92/09 and C-93/09 Schecke and Eifert**”), paragraph 86.

¹¹² Footnote from the Article 65 Decision: Draft Decision, paragraph 435.

Instagram, rather than by e-mail or phone¹¹³. The Draft Decision clearly stated that “[Meta IE] acknowledges that publication of phone and email contact information was not always preferred from the perspective of business account users” because, according to Meta IE “[s]ome businesses also noted that they preferred [...] to communicate with their audience or customers through direct messaging on Instagram rather than traditional means (like phone or email)”¹¹⁴. Despite this, the IE SA failed to take account of such circumstances in its assessment of the necessity requirements and erred in its conclusion that the contact information processing was necessary for the performance of the contract in the present case.

97. The EDPB recalls that within the “contact information processing” there was also a processing operation (occurring for a specific timeframe) consisting in the publication in plain text of the contact information in the HTML source code on the Instagram website. Meta IE highlighted that “business contact information appeared in the HTML source code for Business Accounts for the purpose of providing a “Contact” button on the Web version of Instagram” since “in order for a web browser to render the relevant Instagram Web page, the browser must ‘speak’ to an Instagram Web server”¹¹⁵. The IE SA found an infringement (not disputed by the objections raised) of the principle of data minimisation limited to this “mandatory publication (prior to 7 March 2019) of contact information on the website version of Instagram (in HTML) for all business account users”, since this “had the result that the personal data at issue (i.e. contact information of child users on webpages) was not limited to what was necessary in relation to the purposes for which [Meta IE] processed this specific information”¹¹⁶. As noted by the IE SA, the HTML publication of contact information was not considered necessary by Facebook’s Security Team and was subsequently discontinued¹¹⁷. The EDPB considers that the analysis of the principle of data minimisation (Article 5(1)(c) GDPR) is relevant for the necessity assessment on the basis of Article 6(1)(b) GDPR¹¹⁸. Consequently, the EDPB further finds that such analysis should have complemented the LSA’s assessment on the necessity of the processing for the performance of the contract, with specific regard to the publication of the contact information in the HTML source code on the Instagram website. The EDPB considers that the IE SA could not have concluded that the publication of the contact information of child users in the HTML source code may be regarded as

¹¹³ Footnote from the Article 65 Decision: Draft Decision, paragraph 210.

¹¹⁴ Footnote from the Article 65 Decision: Draft Decision, paragraphs 210 and 238.

¹¹⁵ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions. Paragraph 69.

¹¹⁶ Footnote from the Article 65 Decision: Draft Decision, paragraph 429. As further specified in the Draft Decision, Finding 7 covers the period from 25 May 2018 to November 2020, but does not include the period between July 2019 to August 2020, see Draft Decision, paragraph 525.

¹¹⁷ Footnote from the Article 65 Decision: Draft Decision, paragraph 428: “In particular, when abandoning the HTML publication of contact information in March 2019, a representative with the Facebook Security Team informed Mr Stier ‘After discussing this functionality with the Instagram team we did take steps to remove the contact information from the HTML of the page, since it was not necessary to include in its current form’. As such, [Meta IE]’s submission that this HTML processing was necessary is directly contradicted by the actions and words of the Facebook Security Team. FB-I states that this processing was necessary to provide business accounts to child users, who would otherwise be impeded in promoting their professional activities on Instagram; whereas the Facebook Security Team stated expressly that this processing was not necessary, and stopped this practice immediately when it was brought to its attention.”

¹¹⁸ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 15.

necessary for the performance of the contract between Meta IE and child users.

98. Also, the EDPB takes note of the findings in the Draft Decision that the contact information processing could pose severe risks to the rights and freedoms of child users¹¹⁹. The existence of such risks could have also been considered in the assessment as to whether the processing of the child users' contact information was necessary for the contract.

99. Considering the above¹²⁰ and in light of the specific circumstances of the processing, the EDPB finds that the IE SA could not have concluded in paragraph 115 of the Draft Decision that the contact information processing may be regarded as **necessary** for the performance of a contract between Meta IE and child users.

100. As a consequence, the EDPB finds that **Meta IE could not have relied on Article 6(1)(b) GDPR as a legal basis** for the contact information processing."

121. In its submission of 9 August 2021 responding to the PDD, FB-I contends that the DPC's assessment of purpose in the context of Article 6(1)(b) (i.e. an assessment of whether processing is necessary for the purpose of contractual performance) is essentially equivalent to the assessment of the purpose of processing in the context of Articles 13, 24, 25, and 35 GDPR. For the reasons outlined in paragraph 81 above, I do not accept FB-I's submission in this regard, because greater specificity of purpose is necessary in the context of those provisions, in order that GDPR compliance can be assessed by reference to objective criteria, and in order that data subjects are properly informed as to the characteristics of processing.

Assessment of processing on the basis of Article 6(1)(f) GDPR

122. For this purposes of this Inquiry, I have also considered FB-I's alternative legal basis for the contact information processing under Article 6(1)(f) GDPR. In the Draft Decision, I expressed the view that that the processing meets the requirements of Article 6(1)(f) to the extent that the interests pursued in connection with the contact information processing are legitimate interests of FB-I and other Instagram users, insofar that publication of contact details to the public may be a reasonable and lawful mode by which to promote a professional undertaking or other public initiative.

123. In relation to the necessity of the processing, in that Draft Decision, I also expressed the view that such processing may have been, to an extent, a reasonable means for Instagram users to publish off-platform contact details in some circumstances. In particular, such processing could be regarded as necessary for those business account

¹¹⁹ Footnote from the Article 65 Decision: As set out in Part G.2 of the Draft Decision.

¹²⁰ Footnote from the Article 65 Decision: Paragraphs 80-98 of this Binding Decision.

users who wished to be publicly contactable by email or phone in connection with their professional activities.

124. With regard to the balancing of the legitimate interests against the interests, rights and freedoms of child users (and for the reasons which are addressed in detail elsewhere in this Decision) I expressed the view, in the Draft Decision, that I was not minded to agree with FB-I's analysis of the adequacy of information it provided to child users. Neither did I agree that the security and safety measures implemented by FB-I had the effect of mitigating all relevant risks for child users.

125. Notwithstanding this, I did not dispute FB-I's submission that child users of Instagram may use Instagram in the course of their activities as "*artists, bloggers, celebrities, entrepreneurs...charitable organizations, influencers, musicians, and social activists*", and that these professional purposes may include the publication of contact information in the context of a business account. I further expressed the view that I was satisfied that the rights and freedoms of child users may be adversely impacted should they be "*locked out*" of service elements, or provided with a less complete service in comparison to adult users, in a disproportionate manner. As noted in other contexts¹²¹, such an approach risks interfering with the child's right to express their views fully, their right to freedom of expression and to seek, review and impart information and ideas.

126. With regard to the processing at issue, the balancing of rights and interests takes place in a context of a service offered to millions of child users. A user's capacity to assimilate information, and their digital literacy, will vary from person to person in a way that cannot be predicted solely by the age of the user. Some child users of Instagram may be well informed on the safe use of social media platforms, and may legitimately decide to engage in professional activities on Instagram. Technically literate users may have reasonably expected the public dissemination of their contact information when switching to a business account. Equally, the potential impacts on a child user may vary (for example) depending on whether that user had sufficient technical awareness to use separate modes of contact for their business activities and personal life. I also note that (subject to my below findings) the decision to switch to a business account was elective, and could have benefitted the interests of child users who had a *bone fides* professional purpose to publish off-Instagram contact information.

127. I concluded, in that Draft Decision, that in some circumstances, where the contact information processing occurred in the context of the well-considered professional activities, it is possible that the legitimate interests at issue would not be overridden by the interests or fundamental rights and freedoms of the child user. However, I made it clear that this view was without prejudice to the subsequent analysis and findings

¹²¹ Data Protection Commission – "*Children Front and Centre - Fundamentals for a Child-Oriented Approach to Data Protection*" – Draft version published December 2020 — page 42

elsewhere in the Draft Decision, whereby I addressed specific GDPR obligations of FB-I regarding this processing, and failures in this regard.

128. In conclusion, I indicated my satisfaction that the contact information processing could be lawful on the basis of Article 6(1)(f) GDPR in respect of some of the child users at issue. Accordingly, and for the purpose of section 111(1) of the 2018 Act, and on the basis of the facts of this Inquiry as they were known to me, I proposed to conclude that I was not satisfied that an infringement by FB-I occurred to the extent that it relied on Article 6(1)(f) GDPR as a legal basis for processing personal data of certain child users.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

129. The supervisory authorities of Germany (via Hamburg), Finland, France, Italy, the Netherlands and Norway each raised an objection to the finding proposed under this particular heading.

130. The objections identified various concerns in relation to the assessment of legitimate interests as a legal basis for the contact information processing.

131. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, these matters were included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution process.

132. Having considered the merits of the objections, the Board determined as follows:

“ ...

101. *The EDPB recalls that personal data can be processed on the basis of Article 6(1)(f) GDPR when the processing is necessary for the purposes of the legitimate interests of the controller or of a third party, inasmuch as those interests are not overridden by the interests or fundamental rights and freedoms of the data subjects concerned. In this regard, particular attention should be paid when the data subject is a child¹²².*

102. *The EDPB recalls¹²³ that Article 6(1)(f) GDPR is one of the legal grounds that controllers can rely on for the processing of personal data, as long as the conditions for relying on it are fulfilled¹²⁴.*

103. *As the CJEU has confirmed, Article 6(1)(f) GDPR establishes three cumulative conditions, in order for the processing to be lawful: “first, the pursuit of a*

¹²² Footnote from the Article 65 Decision: Art. 6(1)(f) and Recital 38, GDPR.

¹²³ Footnote from the Article 65 Decision: EDPB Guidelines 8/2020 on the targeting of social media users, version 2.0, adopted on 13 April 2021, paragraph 48.

¹²⁴ Footnote from the Article 65 Decision: See, as well, WP29 Opinion 06/2014 on the notion of legitimate interests, p. 10-11.

legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of [the data subject] do not take precedence”¹²⁵.

a. Existence of a legitimate interest

104. *The EDPB recalls that a legitimate interest can have a legal, economic or non-material nature but needs to be real and present¹²⁶, and not fictitious, for the entity in question: as clarified by the CJEU case law, the legitimate interest must be present and effective at the date of the data processing and must not be hypothetical at that date¹²⁷. The EDPB moreover considers that the interest pursued must be determined in a sufficiently clear and precise manner: the determination and perimeter of the legitimate interest pursued must be clearly identified in order to ensure that it will be properly balanced against the interests or fundamental rights and freedoms of the data subject. In addition, the legitimate interest must also be lawful (i.e., acceptable under the law)¹²⁸. As a general rule, those interests which can be traced back to the law – a legislative measure or a legal principle – can amount to “legitimate” interest.*

105. *As a preliminary matter, the EDPB notes that the DE SAs considered that a legitimate interest cannot exist when the controller relies on it only in case that Article 6(1)(b) GDPR is not applicable to minors on the basis of national law. In the view of the DE SAs, accepting reliance on Article 6(1)(f) GDPR in this situation would be a “circumvention of the corresponding child protection provisions” and “contradicts the purpose of these provisions”¹²⁹. In this respect, the EDPB recalls that, as stated by the WP29, “[a]n appropriate assessment of the balance under [Article 6(1)(f)] (...) may in some cases be a valid alternative to inappropriate use of, for instance, the ground of ‘consent’ or ‘necessary for the performance of a contract’. Considered in this way, [Article 6(1)(f)] presents complementary safeguards compared to the other pre-determined grounds”¹³⁰. Therefore, it does not seem impossible for a controller to rely on Article 6(1)(f) GDPR if, given the specific circumstances of the processing, the requirements enshrined in the GDPR are met. In order to determine whether processing of personal data may rely on Article 6(1)(f)*

¹²⁵ Footnote from the Article 65 Decision: C-13/16 *Rīgas*, paragraph 28.

¹²⁶ Footnote from the Article 65 Decision: EDPB Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020 (hereinafter, “**EDPB Guidelines 3/2019 on video devices**”), paragraphs 18 and 20.

¹²⁷ Footnote from the Article 65 Decision: *TK v Asociația de Proprietari bloc M5A-ScaraA* (Case C-708/18, judgement delivered on 11 December 2019, ECLI:EU:C:2019:1064), paragraph 44.

¹²⁸ Footnote from the Article 65 Decision: See, in this respect, WP29 Opinion 06/2014 on the notion of legitimate interests, p. 25.

¹²⁹ Footnote from the Article 65 Decision: DE SAs objection, p. 5.

¹³⁰ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 10 and 49.

GDPR, data controllers must assess in detail whether the cumulative conditions aforementioned can be met so that the processing of personal data is lawful.

106. In the Draft Decision, the IE SA considered that the legitimate interests pursued are those of Meta IE and other Instagram users, “insofar that publication of contact details to the public may be a reasonable and lawful mode by which to promote a professional undertaking or other public initiative”¹³¹. The IE SA did not specify if it referred to all Instagram users or to a specific type of users. Considering the submissions of the controller, to which the Draft Decision referred in paragraph 109, it appears that the IE SA’s followed the former interpretation (i.e., looking at the interests of all Instagram users).

107. In its submission, Meta IE stated that “the display of business contact information served [Meta IE]’s legitimate interest of creating, providing, supporting, and maintaining innovative products and features that enable people under the age of majority to express themselves, communicate, and engage with information and communities relevant to their interests and build community. The display of business contact information on a Business Account also served the legitimate interest of other Instagram users who sought to engage with such an account”¹³². Therefore, in accordance with Meta IE’s submission, the legitimate interests pursued are connected to the fundamental right to conduct a business and the fundamental right to freedom of expression of Instagram users¹³³. The IE SA seemed to agree with such interpretation¹³⁴, although the IE SA did not specify how it came to such conclusion.

108. The NL SA and the FI SA argued in their objections that the IE SA did not sufficiently assess whether the interests as formulated by Meta IE are sufficiently clear, precise, lawful (i.e., acceptable under the law) and of real existence¹³⁵.

109. As described above, Meta IE described the different interests that it pursued with the processing of personal data at stake. More specifically, Meta IE pursued:

- the legitimate interest of the controller of “creating, providing, supporting, and maintaining innovative products and features that enable people under the age of majority to express themselves, communicate, and engage with information and communities relevant to their interests and build community”, and

¹³¹ Footnote from the Article 65 Decision: Draft Decision, paragraph 118.

¹³² Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 77.

¹³³ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, Appendix 5, section 2.a.

¹³⁴ Footnote from the Article 65 Decision: Draft Decision, paragraph 121.

¹³⁵ Footnote from the Article 65 Decision: NL SA objection, paragraph 28; FI SA objection, paragraph 14.

- *the legitimate interest of a third party (i.e., other Instagram users) to be able to engage with Business Account owners.*

110. *As stated above, the legitimate interest pursued by the controller must be sufficiently clearly articulated and be real and present, corresponding to current activities or to benefits that are expected in the near future¹³⁶. The aforementioned interests the controller claimed to be pursuing via the processing activities at stake were identified and described in a vague fashion. This is especially the case for the second interest mentioned. Therefore, the EDPB has doubts that the legitimate interest argued by Meta IE meets the requirements of being sufficiently specific, despite Meta IE's allegations on the contrary¹³⁷. Therefore, due to the lack of specificity, the EDPB cannot assess whether the interests argued are real and lawful (i.e., acceptable under the law). The EDPB also considers that the evaluation of the existence of the legitimate interest(s) pursued should have been more substantiated in the Draft Decision.*

111. *In any case, the existence of a legitimate interest is only one of the three cumulative conditions that must be met in order to lawfully rely on Article 6(1)(f) GDPR. The EDPB analyses below the two other conditions having regard to the alleged legitimate interests, as described and identified by the controller, in case they were to be considered sufficiently clear, precise, real and lawful (i.e., acceptable under the law).*

b. The necessity of the processing for the purposes of the legitimate interests

112. *As stated above, the concept of necessity has an independent meaning in Union law, which must reflect the objectives of data protection law¹³⁸. The assessment of what is necessary involves a combined, fact-based assessment of the processing for the objective pursued. If there are realistic, less intrusive alternatives, the processing cannot be considered as necessary¹³⁹.*

113. *With regard to Article 6(1)(f) GDPR, the necessity of the processing requires a connection between the processing and the legitimate interest(s) pursued and should not lead to an unduly broad interpretation thereof¹⁴⁰. In this context,*

¹³⁶ Footnote from the Article 65 Decision: See also WP29 Opinion 06/2014 on the notion of legitimate interests, p. 24.

¹³⁷ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 77. .

¹³⁸ Footnote from the Article 65 Decision: C-524/06 *Huber*, paragraph 52

¹³⁹ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019, paragraph 25; Also C-92/09 and C-93/09 *Schecke and Eifert*, paragraph 86. The EDPB considers that the existence of other less intrusive means as part of the assessment of necessity is in line with the CJEU case law and the GDPR, inasmuch as such assessment takes account of the possibility to *effectively* achieve the objectives via other means. In this respect, there is no contradiction between the objections (and the EDPB's position) and the Court of Justice judgement in C-524/06 *Huber*, contrary to what Meta IE argued (Meta IE Article 65 Submissions, paragraphs 78-79).

¹⁴⁰ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 29.

the EDPB recalls that the principle of data minimisation is relevant¹⁴¹. The EDPB notes that the IE SA found an infringement of the principle of data minimisation limited to “the mandatory publication (prior to 7 March 2019) of contact information on the website version of Instagram (in HTML) for all business account users”, since it “had the result that the personal data at issue (i.e. contact information of child users on webpages) was not limited to what was necessary in relation to the purposes for which [Meta IE] processed this specific information”¹⁴². The EDPB considers that such analysis should have complemented the assessment on the necessity of the processing, with specific regard to the HTML publication processing operation, as stated above.

114. In addition, it is relevant to highlight also in this context that when assessing the necessity of a given processing operation, the existence of less intrusive means that would contribute effectively to achieving the interests pursued should be analysed. In this respect, the principle of proportionality should also be taken into account¹⁴³. However, the IE SA did not analyse in the Draft Decision whether other less intrusive means were available to effectively achieve the objectives pursued. In this regard, the existing possibility to contact business account users directly through direct messaging within the platform should have been taken into consideration. In fact, it is clear from the Draft Decision that Meta IE was aware, prior to 4 September 2019, that certain business account users preferred to communicate with their audience through direct messaging on Instagram, rather than by e-mail or phone¹⁴⁴. The IE SA clearly stated that “[Meta IE] acknowledges that publication of phone and email contact information was not always preferred from the perspective of business account users” because, according to Meta IE “[s]ome businesses also noted that they preferred [...] to communicate with their audience or customers through direct messaging on Instagram rather than traditional means (like phone or email)”¹⁴⁵. The IE SA also considered that “it is possible to operate a professional profile without also publishing contact information”¹⁴⁶. Despite this, the IE SA failed to take account of such circumstances for the assessment of the necessity of the contact information processing.

115. Finally, the EDPB notes that the IE SA considered that, in some circumstances, the publication of the contact details of minors may have been necessary in some cases, in particular with respect to those business account users who wished to be publicly contactable by email or phone in connection with their professional activities¹⁴⁷.

¹⁴¹ Footnote from the Article 65 Decision: EDPB Guidelines 3/2019 on video devices, paragraph 29.

¹⁴² Footnote from the Article 65 Decision: Draft Decision, paragraph 429.

¹⁴³ Footnote from the Article 65 Decision: C-92/09 and C-93/09 *Schecke and Eifert*, paragraph 86.

¹⁴⁴ Footnote from the Article 65 Decision: Draft Decision, paragraph 210.

¹⁴⁵ Footnote from the Article 65 Decision: Draft Decision, paragraphs 210 and 238.

¹⁴⁶ Footnote from the Article 65 Decision: Draft Decision, paragraph 353.

¹⁴⁷ Footnote from the Article 65 Decision: Draft Decision, paragraph 119.

116. *The EDPB considers that the approach adopted by the IE SA when assessing the necessity of the processing is substantially erroneous. As stated above, reliance on Article 6(1)(f) GDPR requires that the processing be necessary to achieve the legitimate interests pursued, which, in this case, Meta IE considers to be the interest to conduct its business and the interest of Instagram users to contact business account owners and engage with them¹⁴⁸. The benefits that such processing may bring to the data subject (i.e., in this case, the child business account owners) are not a relevant element for the assessment of necessity of the processing. Article 6(1)(f) GDPR is clear when it states that the legitimate interests are those of the controller or of a third party (and not those of the data subject). Therefore, when assessing the necessity of the processing, the legitimate interests at stake have to be considered with regard to the controller and, if relevant, the third parties concerned (i.e., Meta IE and all Instagram users, in this case).*

117. *Due to the approach adopted by the IE SA, it failed to justify in the Draft Decision why it considered the publication of contact details necessary for the attainment of the purposes of legitimate interests of Meta IE and other Instagram users. In fact, it is apparent from the Draft Decision that Instagram users had other means of communication with business account users that did not significantly diminish the possibility of engaging with those accounts. The availability of other means of communication with business account users is also shown by the fact that certain business account users even preferred to communicate with their audience via direct messaging within the platform and did not want their information to be public. As the IE SA acknowledged “[i]t is also clear that many business account users did not require the publication of personal contact information in order to pursue their professional purposes on Instagram”¹⁴⁹ and that “the requirement to publish contact information was clearly not ‘appropriate’ as of May 2018”¹⁵⁰. This proves with significant certainty that Instagram users could have achieved the alleged legitimate interest of engaging with business account owners even if their contact details were not public and, therefore, Meta IE could also achieve its alleged legitimate interest to create, provide, support and maintain innovative products that enable children to express themselves, communicate and engage with others.*

118. *Therefore, in the view of the EDPB, the IE SA failed to take into account the relevant legitimate interests when performing the assessment of necessity of the processing and, therefore, it should have not concluded¹⁵¹ that the processing may have been necessary in some circumstances.*

¹⁴⁸ Footnote from the Article 65 Decision: See paragraph 109 of this Binding Decision.

¹⁴⁹ Footnote from the Article 65 Decision: Draft Decision, paragraph 429.

¹⁵⁰ Footnote from the Article 65 Decision: Draft Decision, paragraph 433.

¹⁵¹ Footnote from the Article 65 Decision: See Draft Decision, paragraph 119.

119. *For the reasons described above, the EDPB considers that there are sufficient elements to raise significant doubts on the necessity of the publication of the contact information of child users for the purposes of the legitimate interests pursued.*

120. *In any case, even if the necessity of the processing could be established under some circumstances, in order to lawfully rely on Article 6(1)(f) GDPR as a legal basis for the processing, there is a need to ensure that the interests and fundamental rights and freedoms of the data subjects do not override the legitimate interests pursued.*

c. The balancing exercise

121. *When a controller intends to rely on Article 6(1)(f) GDPR, it has to evaluate the risks of intrusion on the data subject's rights. In this respect, the decisive criterion is the intensity of the intervention for the rights and freedoms of the individual¹⁵². The EDPB has previously stated that intensity can inter alia be defined by the type of information that is gathered, the scope, the number of data subjects concerned, the situation in question, the actual interests of the group of data subjects, the existence of alternative means, as well as by the nature and scope of the data assessment¹⁵³. The reasonable expectations of the data subject at the time and in the context of the processing shall also be considered¹⁵⁴. In this regard, the EDPB recalls that the age of the data subject may be one of the factors to take into account in the context of the balancing of interest¹⁵⁵.*

122. *The objective of the balancing of interests is to understand the impact of the processing on the data subjects, in order to properly conclude whether their interests or fundamental rights and freedoms override the legitimate interests of the controller. The purpose is not to prevent any negative impact on the data subject, but to prevent a disproportionate impact¹⁵⁶. Such impact encompasses the different ways in which an individual may be affected - positively or negatively - by the processing, and should address any possible (potential or actual) positive and negative consequences of such processing¹⁵⁷. These consequences may include potential or future decisions or actions by third parties or fear and distress that the data subject may experience when losing control over personal information, for example through exposure on the internet¹⁵⁸. The key elements to assess the impact*

¹⁵² Footnote from the Article 65 Decision: EDPB Guidelines 3/2019 on video devices, paragraph 32.

¹⁵³ Footnote from the Article 65 Decision: EDPB Guidelines 3/2019 on video devices, paragraph 33.

¹⁵⁴ Footnote from the Article 65 Decision: EDPB Guidelines 3/2019 on video devices, paragraph 36.

¹⁵⁵ Footnote from the Article 65 Decision: Case C-13/16 *Rigas*, paragraph 33; and WP29 Opinion 06/2014 on the notion of legitimate interests, p. 40.

¹⁵⁶ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 41.

¹⁵⁷ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 37.

¹⁵⁸ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 37.

are the likelihood that the risk materialises, on one hand, and the severity of the consequences on the other one¹⁵⁹. The EDPB underlines that safeguards play a special role in reducing any undue impact on the data subject. In order to ensure that the interests and fundamental rights and freedoms of data subjects do not override the legitimate interests pursued, the safeguards in question must be adequate and sufficient, and must unquestionably and significantly reduce the impact on data subjects¹⁶⁰.

123. The assessment should also take into account the measures that the controller plans to adopt in order to comply with its obligations, including in terms of proportionality and transparency¹⁶¹. The relationship between the balancing test, transparency and the accountability principle has already been underlined by the WP29, which considered it “crucial” in the context of Article 6(1)(f) GDPR¹⁶². In this regard, the EDPB recalls that, if the controller hides important information to the data subject, it will not fulfil the requirements of reasonable expectations of the data subject and an overall acceptable balance of interests¹⁶³.

124. In the Draft Decision, the IE SA disagreed with Meta IE’s analysis of the adequacy of the information provided to child users and the security and safety measures implemented, which, in the view of the IE SA, did not mitigate all relevant risks for child users¹⁶⁴. In fact, the insufficiency of the measures led the IE SA to conclude that “there are possible and severe risks associated with the two forms of processing which are the subject of this Inquiry; these risks are primarily related to possible communication between child users and dangerous individuals, both on and off the Instagram platform (...). I am also satisfied that the measures and safeguards implemented by [Meta IE] (in the form of account options, tools and information) were not adequate with regard to the specific processing operations at issue” since they “did not adequately mitigate the risk of communication between dangerous individuals and child users. Accordingly, I do not share [Meta IE]’s view that the processing at issue did not result in high risks to the rights and freedoms of child users”¹⁶⁵. The IE SA also considered that the changes to the processing in July and September 2019 “reduced but did not adequately mitigate the risks for child users in connection with the processing”¹⁶⁶. Meta IE argued that

¹⁵⁹ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 38.

¹⁶⁰ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 31.

¹⁶¹ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 33 and 41.

¹⁶² Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 43.

¹⁶³ Footnote from the Article 65 Decision: See WP29 Opinion 06/2014 on the notion of legitimate interests, p. 44.

¹⁶⁴ Footnote from the Article 65 Decision: Draft Decision, paragraph 120.

¹⁶⁵ Footnote from the Article 65 Decision: Draft Decision, paragraph 356

¹⁶⁶ Footnote from the Article 65 Decision: Draft Decision, paragraph 389.

neither the CSAs nor the IE SA gave “due weight to the other half of the balancing test to mitigate and/or negate” the risks to the data subjects¹⁶⁷. Therefore, the EDPB disagrees with the view of Meta IE and considers that the IE SA on the assessment of the risk is accurate. The EDPB also underlines that it is possible to accommodate the objective of effectively reducing the risk for children while ensuring their right to freedom of expression, by implementing appropriate safeguards and measures¹⁶⁸.

125. The IE SA also addressed the lack of transparency regarding the information on the publication of the contact details. In this respect, the IE SA stated in the Draft Decision that “[Meta IE] facilitated the publication of phone and email contact information for children as young as 13, using a streamlined account switching process which automatically completed certain information for the user, without warning child users that publication of their personal contact information may result in high risks to their rights and freedoms”¹⁶⁹. Therefore, taking into account both the assessment of the risk and the mitigating measures, as well as the lack of information provided, the IE SA concluded that “the contact information processing by [Meta IE] (both before September 2019, and after) results in high risks to the rights and freedoms of child users, for the purposes of Article 35(1) GDPR”¹⁷⁰.

126. As mentioned above, the transparency of the information provided has an impact on the reasonable expectations of the data subjects. Likewise, adequate and sufficient additional safeguards are those that unquestionably and significantly reduce the impact on data subjects. These are important elements to take into account in the assessment of the balancing of interests. However, despite acknowledging the lack of proper measures and information, and the severe risks that this creates for child users, when analysing the balancing exercise to verify whether Meta IE could rely on Article 6(1)(f) GDPR the IE SA only concluded that, in some circumstances, it is possible that the legitimate interests would not be overridden by the interests or fundamental rights and freedoms of the child user¹⁷¹. In addition, despite the lack of proper information, the IE SA concluded that technically literate users may have expected the publication, regardless of their age¹⁷². The EDPB finds particularly problematic that, despite the risks of the processing, recognised by Meta IE itself¹⁷³, the publication of contact details

¹⁶⁷ Footnote from the Article 65 Decision: Meta IE Article 65 Submissions, paragraph 10.

¹⁶⁸ Footnote from the Article 65 Decision: See Draft Decision, paragraph 353.

¹⁶⁹ Footnote from the Article 65 Decision: Draft Decision, paragraph 389 (emphasis added).

¹⁷⁰ Footnote from the Article 65 Decision: Draft Decision, paragraph 389 (emphasis added).

¹⁷¹ Footnote from the Article 65 Decision: Draft Decision, paragraph 123. In particular, the IE SA referred to situations “where the processing occurred in the context of well-considered professional activities”.

¹⁷² Footnote from the Article 65 Decision: Draft Decision, paragraph 122.

¹⁷³ Footnote from the Article 65 Decision: Draft Decision, paragraph 381; Meta IE Article 65 Submissions, Appendix 5, sections 4.2.a and 4.2.b.

of child users was mandatory until 4 September 2019. In fact, child users were not even informed of such publication, since the Option Screen only stated that “these contact options will be linked to your business profile”¹⁷⁴. Even though the screen included a note at the end stating that “people will be able to email, call and get directions to your business [...]”, it did not specify that it was because of the publication of the information. In the view of the EDPB, it is not reasonable to expect that a normal user, let alone a child, even if technically literate, could deduce from such a vague statement that publication of their information would take place and that it would allow any type of person (including persons with whom they had had no contact or link) to contact them directly. In fact, as the IE SA noted, the term “will be able” may have been understood by the child users as a conditional indication that an additional contact-publication feature could be implemented optionally by the user¹⁷⁵.

127. Taking the above into consideration, the EDPB is of the view that the IE SA did not properly assess the impact of the processing when performing the balancing exercise. In fact, the IE SA only took into account the positive consequences of the processing¹⁷⁶, whereas it failed to give proper weight to all the other relevant elements and the risks it had itself identified.

128. Therefore, the EDPB considers that, regarding the publication of the contact information of child users **prior to 4 September 2019**, the legitimate interests pursued were overridden by the interests and fundamental rights and freedoms of child users. The EDPB comes to this conclusion given the severe risks identified by the IE SA, the lack of appropriate measures to address those risks, the lack of proper information to data subjects regarding publication and its consequences and the impossibility to opt-out from the publication. All these elements combined tip the balance in favour of the interests and fundamental rights and freedoms of the data subjects.

129. With regard to the processing of personal data of child users **after 4 September 2019**, the EDPB notes that the Option Screen stated that the contact information would be displayed publicly in the profile of the users “so people can contact you”¹⁷⁷. This change in the wording could have allowed child users to understand that any person could contact them as their details would be publicly available¹⁷⁸. In addition, child users were given the option to opt-out from the publication of their contact details. The availability of a

¹⁷⁴ Footnote from the Article 65 Decision: Draft Decision, paragraph 42, Figure 1.

¹⁷⁵ Footnote from the Article 65 Decision: Draft Decision, paragraphs 184 and 185.

¹⁷⁶ Footnote from the Article 65 Decision: See Draft Decision paragraph 121, where the IE SA assessed the potential negative consequences if the processing didn’t take place.

¹⁷⁷ Footnote from the Article 65 Decision: Draft Decision, paragraph 42, Figure 2.

¹⁷⁸ Footnote from the Article 65 Decision: See also Draft Decision, paragraph 206.

well-designed opt-out option without the need for any justification to exercise it and the relationship between the balancing test and transparency are crucial for the balancing exercise under Article 6(1)(f) GDPR. In fact, in those cases in which the balance is difficult to strike, a well- designed and workable mechanism for opt-out could play an important role in safeguarding the rights and interests of the data subjects¹⁷⁹. In this regard, it is relevant to bear in mind the finding of the IE SA in the Draft Decision that the information provided to child users by Meta IE after 4 September 2019 in the course of the business account switching process was in compliance with Articles 12(1), 13(1)(c) and 13(1)(e) GDPR (Finding 3 in the Draft Decision)¹⁸⁰.

130. This being said, the EDPB finds that these elements are not sufficient to change the outcome of the balancing test in light of the aforementioned considerations. This is especially the case because of the high risk resulting from the publication of contact details as explained above in paragraph 124 and of the fact that children were not warned about such risks. These circumstances were not affected by the changes brought as of 4 September 2019 and thus these changes were not sufficient to change the outcome of the balancing test.

131. On the basis of the above, the publication of the contact information of child users prior to and after 4 September 2019 did not meet the requirements under Article 6(1)(f) GDPR, since the interests and fundamental rights and freedoms of the data subjects overrode the alleged legitimate interests pursued.

*132. Considering the EDPB's conclusion in paragraphs 118-119 and, especially, 131 above, it is the view of the EDPB that Meta IE **could not rely on Article 6(1)(f) GDPR for the contact information processing since the processing was either unnecessary or, if it were to be considered necessary, it did not pass the balancing test.***"

Conclusion and Finding

133. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6) GDPR, this Decision finds that FB-I could not have relied on either Article 6(1)(b) or 6(1)(f) GDPR as the legal basis for the contact information processing. As FB-I sought to rely on Article 6(1)(b) and/or 6(1)(f) GDPR as the legal basis for such processing, this Decision find that FB-I have infringed Article 6(1) GDPR.

¹⁷⁹ Footnote from the Article 65 Decision: WP29 Opinion 06/2014 on the notion of legitimate interests, p. 45.

¹⁸⁰ Footnote from the Article 65 Decision: Draft Decision, paragraph 206.

Finding 13

I find that FB-I could not have relied on either Article 6(1)(b) or 6(1)(f) GDPR as the legal basis for the contact information processing.

Accordingly, I find that contact information processing by FB-I infringed Article 6(1) GDPR.

F. Assessment of FB-I's Compliance with Articles 5(1)(a), 12 and 13 GDPR

F.1 Compliance with Articles 5(1)(a), 12(1), and 13 GDPR

134. The GDPR requires that personal data must be processed *“lawfully, fairly and in a transparent manner in relation to the data subject”*¹⁸¹. Specific GDPR provisions are contained in Articles 12(1) and 13 GDPR regarding the information to be provided to data subjects. Article 12(1) GDPR addresses the quality of information to be provided to data subjects, as follows:

“The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14...to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.”

135. FB-I did not provide separate child-specific sources of information (for the purposes of Articles 13 and 14); instead FB-I contends that it tailored the information provided to all users in such a way that it could be easily understood by child users. Accordingly, FB-I's information resources on processing of personal data (e.g. the Data Policy) must be regarded as *“addressed specifically to a child”* for the purposes of Article 12(1) GDPR.

136. Article 13(1) GDPR provides as follows:

“Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

...

*(c) the **purposes of the processing** for which the personal data are intended...;*

...

¹⁸¹ Article 5(1)(a) GDPR

(e) the recipients or **categories of recipients** of the personal data, if any;”
(emphasis added)

137. The WP29 has published Transparency Guidelines¹⁸², which were subsequently endorsed by the EDPB in May 2018.

138. Following the Statement of Issues, this Decision considers whether FB-I has complied with **four** transparency obligations under the GDPR. This Decision does not consider FB-I’s compliance with obligations under Articles 12(1) or 13 in connection with FB-I’s legal basis for processing under Article 6 GDPR.

139. The **first** transparency obligation concerns whether FB-I failed to provide child users with information (in a concise, transparent, intelligible and easily accessible form, using clear and plain language), regarding the **purposes** of the public-by-default processing described in Part C.3 of this Decision, as required under Articles 12(1) and 13(1)(c) GDPR.

140. In this regard, FB-I provided the following information to its child users regarding default account settings;

- The primary source of information on processing by FB-I is the Data Policy. Both the 2018 Data Policy and 2020 Data Policy contain a section titled “*Sharing on Facebook Products*”, which states “*When you share and communicate using our Products, you choose the audience for what you share*”. This section further states:

“Public information can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your public profile on Facebook; and content you share on a Facebook Page, public Instagram account or any other public forum, such as Facebook Marketplace”

- The phrase “*public Instagram account*” in the above extract from the Data Policy contained a hyperlink¹⁸³ to a separate information webpage contained as part of the Instagram Help Center, titled “*How do I set my Instagram account to private so that only approved followers can see what I share?*”. This webpage states:

“By default, anyone can see your profile and posts on Instagram. You can make your account private so that only followers you approve can see what you share. If your account is set to private, only your approved followers will see your photos or videos on hashtag or location pages.” (emphasis added)

¹⁸² Guidelines on transparency under Regulation 2016/679, WP 260 rev.01

¹⁸³ <https://help.instagram.com/448523408565555?ref=dp>

- The *“How do I set my Instagram account to private so that only approved followers can see what I share?”* webpage in the Instagram Help Center sets out the steps to be taken by a user to switch their account to private. The process for switching to a private account is also described in additional informational resources created by FB-I for child users and parents.
- The 2018 Data Policy also contained a second hyperlink¹⁸⁴ to an Instagram Help Center webpage titled *“Controlling Your Visibility”*, which contained information on switching to a private account.

141. The **second** GDPR transparency obligation concerns whether, prior to 4 September 2019, FB-I failed to provide child users with information (in a concise, transparent, intelligible and easily accessible form, using clear and plain language), as required under Articles 12(1), 13(1)(c) and 13(1)(e) GDPR regarding:

- (1) the **purposes** of processing email and phone contact information of child users prior to 4 September 2019 (as described in Part C.3 of this Decision)
- (2) the **categories of recipients** of email addresses and phone numbers of child users (as described in Part C.3 of this Decision) as processed by FB-I prior to 4 September 2019

142. The relevant Facebook Data Policy regarding this issue is the 19 April 2018 version. This Data Policy did not include specific information on the requirement to publish email and/or phone numbers in the context of business accounts.

143. In order to switch to a business account, child users would navigate to the “Settings” section of the Instagram application, and would then select the “Account” section, which contained a link to the “Switch to Business Account” process. The user was subsequently shown a number of information and option screens as part of the switching process. These screens included a preliminary information screen on the use of contact information, as follows:

¹⁸⁴ The text that contained this hyperlink stated *“Learn more about what information is public and how to control your visibility on...Instagram”*

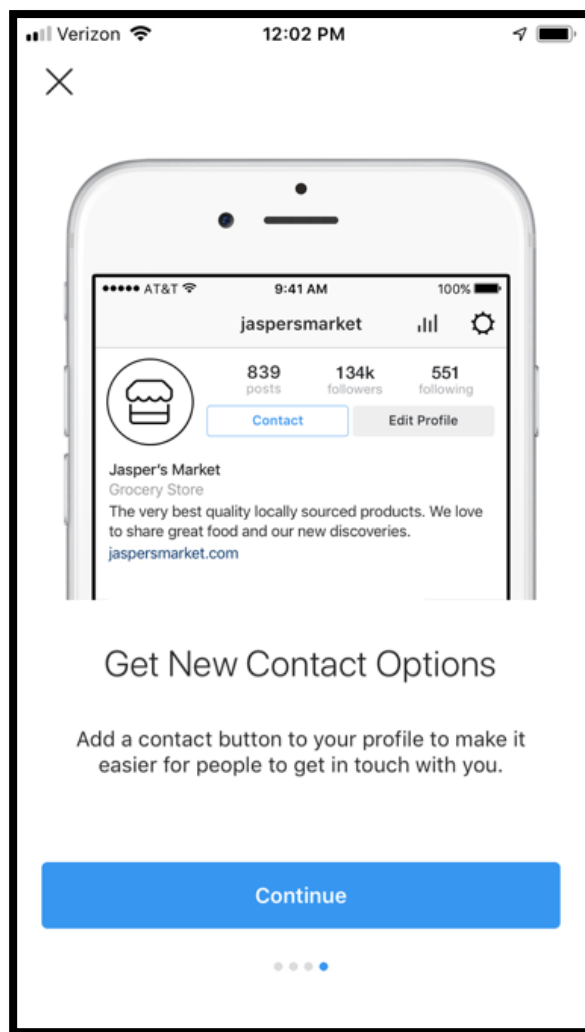
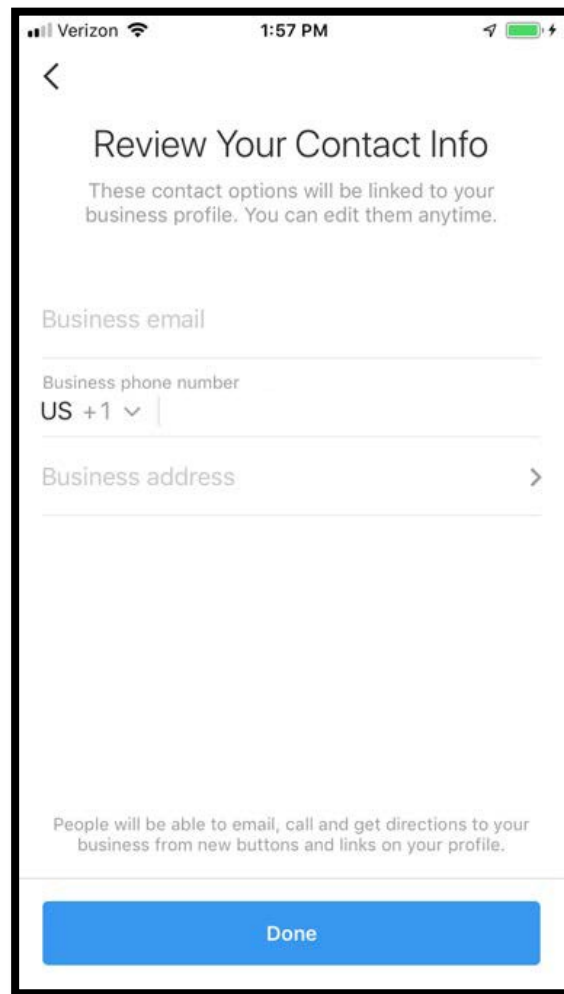


Figure 3 - Pre-September 2019 Information Screen, Appendix J to FB-I's Submission of 27 October 2020

144. Depending on whether the user had a pre-existing Facebook account, they were then shown one of two possible contact information screens, as follows:



The screenshot shows a mobile application interface for reviewing contact information. At the top, the status bar displays 'Verizon', signal strength, Wi-Fi, the time '1:57 PM', and battery level. The app interface has a back arrow in the top left. The title 'Review Your Contact Info' is centered, followed by a subtitle: 'These contact options will be linked to your business profile. You can edit them anytime.' Below this are three input fields: 'Business email', 'Business phone number' (with a dropdown menu showing 'US +1'), and 'Business address' (with a right-pointing chevron). At the bottom, a blue button labeled 'Done' is centered. A small note at the bottom of the form states: 'People will be able to email, call and get directions to your business from new buttons and links on your profile.'

Figure 4 - Pre-September 2019 Information Screen for users with a connected Facebook account, Appendix J to FB-I's Submission of 27 October 2020

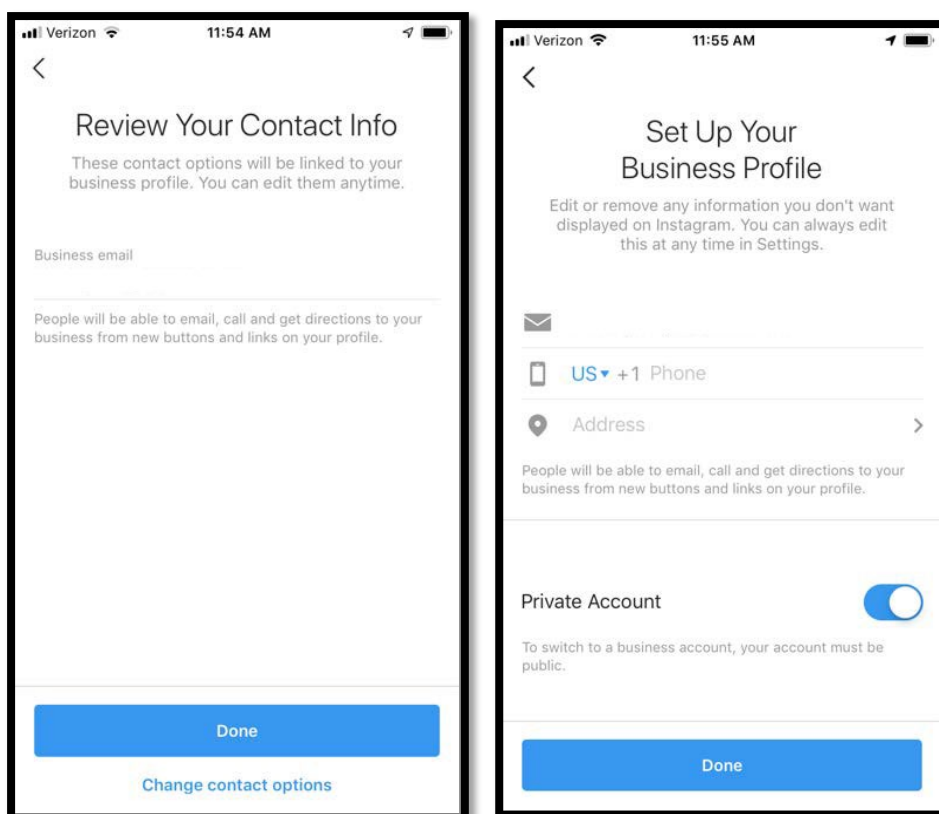


Figure 5 - Pre-September 2019 Contact Information Screens for users without a connected Facebook account, Appendix J to FB-I's Submission of 27 October 2020

145. The **third** transparency obligation concerns whether, after 4 September 2019, FB-I failed to provide child users with information (in a concise, transparent, intelligible and easily accessible form, using clear and plain language), as required under Articles 12(1), 13(1)(c) and 13(1)(e) GDPR regarding:

- (1) the **purposes** of processing email and phone contact information of child users in the context of business accounts (as described in Part C.3 of this Decision)
- (2) the **categories of recipients** of email addresses and phone numbers of child users, as processed in the context of business account (as described in Part C.3 of this Decision)

146. The relevant Data Policy regarding this issue is the 21 August 2020 version. This Data Policy does not include specific information on the facility to publish email and/or phone numbers in the context of business accounts.

147. In order to switch to a business account, child users would navigate to the “Settings” section of the Instagram application, and would then select the “Account” option, which contains a link to the “Switch to Professional Account” process. The user was subsequently shown a number of information and option screens as part of the process.

These screens included a preliminary information screen on the use of contact information, as follows:

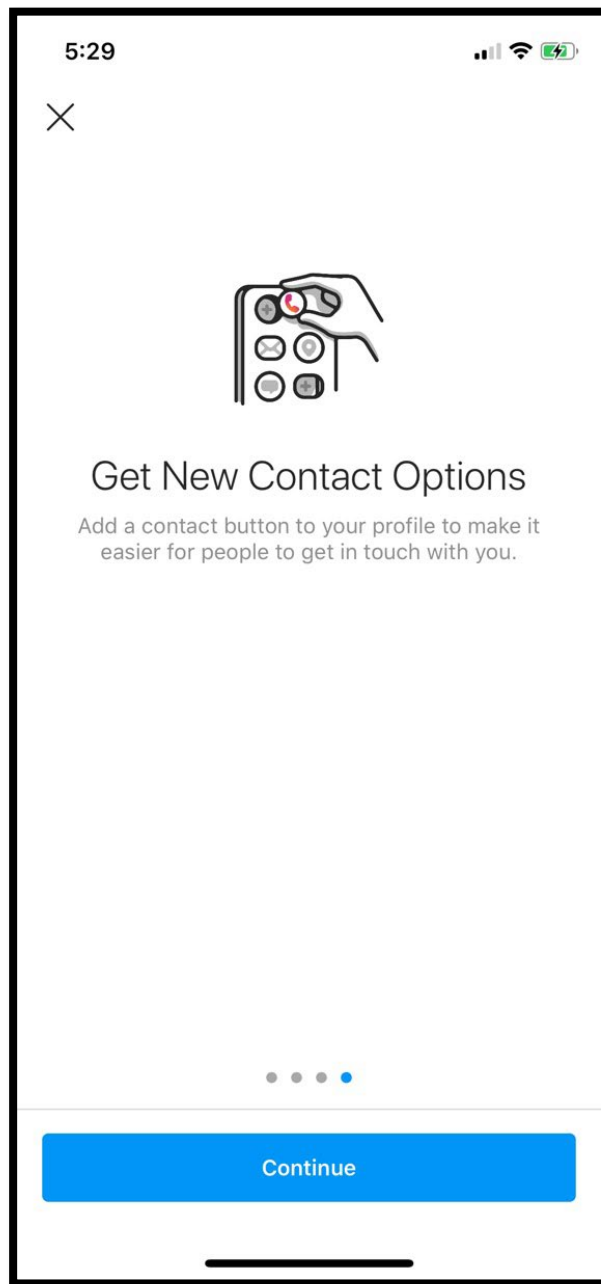


Figure 6 - Contact Information Screen, Appendix I to FB-I's Submission of 27 October 2020

148. When switching to a professional account, FB-I made a recommendation to the user as to whether a “creator account” or a “business account” would be appropriate, based on a professional category selected by the user. Where FB-I suggested a creator account, the user could disregard FB-I’s suggested account type, by manually selecting “business account” instead. Where a user switches from a personal account to a business account,

they are presented with the following option screen regarding the use of their contact information:

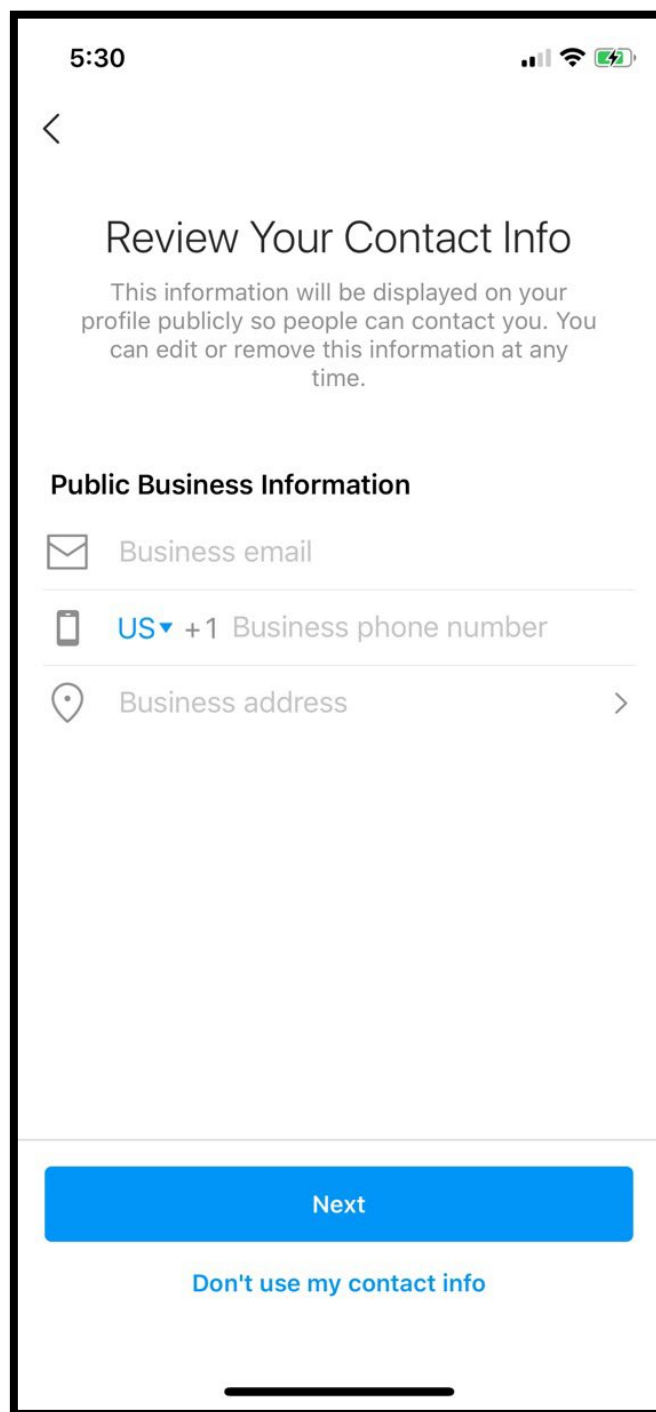


Figure 7 - Contact Information Option Screen, Appendix I to FB-I's Submission of 27 October 2020

149. The **fourth** transparency obligation concerns whether FB-I failed to adequately notify child users of the removal (on 4 September 2019) of the requirement to publish contact information on business profiles (as required in order for processing to be fair and transparent under Article 5(1)(a) GDPR).

150. After 4 September 2019, business account users were provided with the ability to remove their contact information from their profile page, using the “edit profile” option. On 18 October 2019, FB-I published an Instagram Help Centre webpage titled “*Edit Your Business Information on Instagram*”¹⁸⁵, and subsequently published a blog post about updates to business accounts.

F.2 Submissions of FB-I regarding transparency

151. In describing its overall approach to transparency and the provision of information to its users, FB-I states that its safety, privacy, and security tools and resources include¹⁸⁶:

“...dedicated informational resources provided for Teens and parents, including an easily understandable privacy notice (i.e., the Data Policy, which was presented to the Commission’s supervisory team and discussed prior to its launch), Help Centre pages focusing on user-friendly explanations of tools and functionalities available to Teens, and a Parents Guide and Parents Portal with helpful information so that parents can talk to their Teens with knowledge about the product.”

152. FB-I also states:

“while [the above sources of information] are “static” forms of information, in the sense that they can be accessed at any time, Facebook Ireland also utilises dynamic in-product notifications and tips to highlight new tools or features available to Users, including Teens.”

153. FB-I further submits¹⁸⁷ that its Data Policy has been drafted specifically to be understood by child users, as follows:

“...the language in the Data Policy is clear, concise, and intelligible, so it can be understood by Users of all ages, including Teens. In those circumstances, while the Data Policy is intended for all Users, it is also designed to be appropriate for Teen Users...As explained in its First Submission, Facebook Ireland has designed all aspects of the Instagram Service with Teens specifically in mind -- and this includes the manner in which it provides relevant privacy information.”

154. With regard to the **first** transparency obligation under consideration, concerning the public-by-default processing, FB-I submitted¹⁸⁸:

“Facebook Ireland provides information about what it means to have public audience settings by default to all Users, including Teens, before they complete the registration process to create a personal account. During registration, Users are presented with

¹⁸⁵ <https://help.instagram.com/529483457260403>, Appendix O to FB-I’s submission of 27 October 2020,

¹⁸⁶ FB-I’s submission of 18 December 2020, paragraph 4

¹⁸⁷ FB-I’s submission of 18 December 2020, paragraph 14

¹⁸⁸ FB-I’s submission of 18 December 2020, paragraph 11

the Terms of Use, Data Policy, and Cookies Policy. The Data Policy which is publicly accessible at any time, including before a User decides to register for an Instagram account, directly links to a page explaining that “[b]y default, anyone can see your profile and posts on Instagram.” This link is located within a section of the Data Policy prominently labeled, “Public information,” where Facebook Ireland informs Users in easy-to-understand language about how public information may be shared, including that “content you share on a . . . <public Instagram account>” is public information.

155.FB-I further submits that it has adopted a layered approach¹⁸⁹ to the provision of information to child users. FB-I contends that Articles 12 and 13 prescribe only the “*content of the information*” to be provided to data subjects, and not the “*means or method*”. FB-I submits that Article 12, in particular, contains only “*broad principles*” on the mode of information provision, which do not fetter the controller’s discretion as to how information is provided¹⁹⁰. FB-I submits that the Data Policy has been drafted in such a way that it can be understood by child users of Instagram (i.e. persons between the age of 13 and 17). FB-I states that it explained which information is public on Instagram, and how certain information can be made private by users¹⁹¹.

156.With regard to the **second** and **third** transparency obligations under consideration, concerning the publication of contact information, FB-I submitted¹⁹² that relevant information on processing was and is provided to child users in the course of the account switching process. FB-I submits:

“...it is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices. This is what Facebook Ireland does in connection with the public display of contact information in relation to Business Accounts, and it considers it is appropriate to do, given that most Users do not use the Business Account functionality and the information provided will therefore not be relevant for them.”

157.In particular, FB-I contends that the information and option screens which were shown to users during the processing of switching to a business account provided sufficient information to child users on this form of processing.

158.With regard to the **fourth** transparency obligation under consideration, (concerning whether FB-I provided existing business account users with updated information in September 2019), FB-I submitted as follows:

¹⁸⁹ FB-I’s submission of 18 December 2020, paragraph 11

¹⁹⁰ FB-I’s submission of 18 December 2020, paragraph 13

¹⁹¹ FB-I’s submission of 18 December 2020, paragraph 15 to 18

¹⁹² FB-I’s submission of 18 December 2020, paragraphs 39 to 41

“...Facebook Ireland updated its Help Centre on 18 October 2019 to note that the display of a contact detail is optional. For example, see the Help Centre article entitled “Edit Your Business Information on Instagram”. The Help Centre article explained to users that “[y]ou can edit your professional account's Page, business category, and contact information directly from the Instagram app....

Facebook Ireland also published a blog post entitled “New and Updated Tools for Businesses” on 20 December 2019, which – among other information – explained that it “recently launched new features to help businesses better-understand their community and better-control their presence on Instagram.” The blog post highlighted “Flexible Profile Displays”, noting that a user may “Share the profile information that works best for your business. With this feature, you have the option to hide contact information ... on your profile. Learn how to edit your information in our <Help Centre>”.

In addition, as noted above, any user with a Business Account can click on the “Edit Profile” button directly from their profile at any time, where they will see the ability to edit their “Profile Display”, including the option to toggle off the display of contact information.

F.3 Analysis and findings of the DPC

Consideration of first transparency obligation

159. I have first considered whether (as of the time of commencement of this Inquiry) FB-I provided child users with information as required under Articles 12(1) and 13(1)(c) GDPR, in connection with the public-by-default processing of personal data. Article 13(1)(c) requires the provision of specific information to data subjects under the GDPR – i.e. information on the **purposes** of processing for which personal data are intended. Article 12(1) places conditions on the quality of the information provided to data subjects – it must be provided to the data subject *“in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for **any information addressed specifically to a child**”*. It must be noted that the Facebook Data Policy and Instagram Help Centre (and applications settings) are addressed to Instagram users as young as 13.

160. Recital 39 to the GDPR further states *“In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data”* and *“Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing”*.

161. The purpose of processing refers to the **reasons why** a data controller such as FB-I is conducting certain operations on personal data. In my view, FB-I’s processing of

Instagram users' social media posts has two separate and distinct **purposes**, depending on whether the user has a public account or a private account. The purpose of processing social media posts in the case of a public account is to share that content with *"anyone, on or off"*¹⁹³ Instagram. The purpose of processing in the case of a private account is categorically different; it is to share content only to those Instagram users that have been approved by the user.

162. By opting to make accounts of newly-registered child users "public" by default, FB-I effectively determined a particular **purpose** of processing on behalf of a user (subject to the intervention of the user). This is relevant from the perspective of Articles 12(1) and 13(1)(c) because by deciding to set accounts of child users to public by default, an obligation arose on the part of FB-I to provide information (at the time of collection of the user's data) on the specific **purpose** of the processing associated with public accounts.

163. FB-I contends that it relies on both static sources of information (such as the Data Policy), and dynamic sources of information (pop-up notices), in order to provide information to users. Notwithstanding this, it is conspicuous that prior to 2021, the user registration process¹⁹⁴ for persons aged between 13 and 17 did not contain any information about the difference between public accounts and private accounts, nor was there an option during registration to select the type of account preferred by the user. As can be seen from FB-I's subsequent modification of the registration process to include an option screen for account types, it would appear to be technically simple to present this information to new users. Despite this, prior to 2021, children could set up Instagram accounts without any "dynamic" information notice concerning FB-I's default processing purpose for social media content. While FB-I was not required to provide Article 13 information specifically as part of the user registration process, it would have been an apt mode of information provision to describe the purpose of processing for the default user account at this point in time.

164. The Instagram registration process¹⁹⁵ included, on the final screen, text which read *"...learn how we collect, use and share your data in our Data Policy..."*. In turn, the relevant section¹⁹⁶ of the Data Policy concerning data sharing stated *"[w]hen you share and communicate using our Products, you choose the audience for what you share"*. This statement, although not inaccurate, omits to mention that in the case of Instagram, FB-I had made a prior choice on behalf of users as to what information would be shared by default, unless the user intervened to make a different choice. The same section of the Data Policy stated that *"content you share on a...public Instagram account"* can be *"seen*

¹⁹³ Facebook Data Policy, section titled "Sharing on Facebook Products", subsection titled "Public Information"

¹⁹⁴ FB-I's submission of 27 September 2020, Appendix K

¹⁹⁵ FB-I's submission of 27 October 2020, Appendix K

¹⁹⁶ Facebook Data Policy of 19 April 2018, section titled *"People and accounts you share and communicate with"*

by anyone, on or off our Products, including if they don't have an account". This section concludes by inviting the user to *"Learn more about what information is public and how to control your visibility..."* by accessing additional parts of the Instagram Help Centre. What is absent from the Facebook Data Policy is any reference to the fact that FB-I has pre-selected a specific processing purpose for sharing Instagram users' content (public-by-default).

165. FB-I provided hyperlinks from the Data Policy to specific parts of the Instagram Help Center concerning the private account setting¹⁹⁷. In the Instagram Help Center, FB-I acknowledges that *"[b]y default, anyone can see your profile and posts on Instagram"*, and outlines the steps for switching to a private account. Information on how to set an account to "private" can also be accessed through other parts of the Instagram Help Centre, such as the "Blocking People" section.

166. I further note that the Instagram Parent's Guide¹⁹⁸ discusses the differences between public and private accounts, stating *"There are a number of tools that you can share with your teen to give them more control over their digital identity and footprint. One of the first things you want to talk about with your teen is whether their account is going to be public or private"*. The Parent's Guide made no reference to the fact that a child's account would be public unless the user intervened.

167. FB-I purports to provide information on a layered basis, across a number of documents. I have therefore considered the cumulative effect of information provided by FB-I to child users of Instagram. However, I do not accept FB-I's submission that Articles 12 and 13 GDPR prescribe only the *"content of the information"* to be provided to data subjects, and not the *"means or method"*. I agree that Article 12(1) GDPR does not prescribe standard formats or practical arrangements to be adopted. However, the conditions of Article 12(1) concerning the form and quality of information are such that the practical means and methods adopted by a controller may be found to be inadequate transparency measures, and contrary to the GDPR, where for example information is provided in a way that is unclear or unintelligible.

168. With regard to its obligations under Articles 12(1) and 13(1)(c) GDPR, I am satisfied that FB-I provided child users with information on the distinct purposes of processing social media content in connection with public accounts and private accounts. In particular, the Instagram Help Centre webpage acknowledged the default processing purposes implemented by FB-I, and informed users as to how they could change to a private

¹⁹⁷ Instagram Help Center webpage titled "How do I set my Instagram account to private so that only approved followers can see what I share?" available at <https://help.instagram.com/448523408565555?ref=dp>

¹⁹⁸ FB-I's submission of 27 September 2020, Appendix G

account. In this way, FB-I can be said to have complied with the formal requirements of Article 13(1) GDPR, as a standalone provision.

169. What is less clear is whether this information was provided *“in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.”*

170. In this regard, I note that the Transparency Guidelines state¹⁹⁹:

“It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice.

...the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject’s rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.”

171. I also note in this context Recital 39 to the GDPR, which states that the purposes of processing should be explicit, and data subjects should be made aware of the risks, rules and safeguards in relation to processing. I also note the content of Recital 38 GDPR, which recalls that *“[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data”*.

172. In this case, FB-I did not provide information on the purpose of public-by-default processing during the Instagram account registration process. Furthermore, the Data Policy failed to provide explicit information on the specific purpose of processing, which FB-I had adopted by default in the case of child users of Instagram. The required information was provided subsequently in the online Instagram Help Centre, and referred to in other Guides provided by Instagram.

FB-I’s submissions in response to the PDD

173. In its submission of 9 August 2021, FB-I contends²⁰⁰ that the GDPR does not prescribe the *“means, format, modality (or) method”* of information provided to data subjects. FB-I submits that controllers have flexibility in this regard, taking into account *“the user experience of the particular service at issue, the device used to access such service, and*

¹⁹⁹ Guidelines on transparency under Regulation 2016/679, WP260 rev. 01, page 19

²⁰⁰ FB-I’s submission of 9 August 2021, paragraphs 33 to 36

the user journey, as well as limitations of such factors". FB-I also submits that a layered privacy statement is appropriate in the online context.

174. FB-I submits that the approach adopted in the PDD was incorrect, for the following four reasons:

- First, FB-I submits that it was not required to provide granular information on the purposes of processing as part of the Instagram registration process. FB-I contends that it would be contrary to EDPB guidance to provide such information directly as part of registration, because the EDPB has recommended²⁰¹ a layered approach to online privacy policies. FB-I further submits that in other Inquiries, the DPC has adopted the position that the content of specific layers of a privacy policy is not a material concern in the assessment of Article 12(1) GDPR. FB-I submits that the layered approach it adopted (as described above at paragraphs 163 to 166) was sufficient to meet the requirements of Article 12(1).
- Second, FB-I submits that the Data Policy, and not the Instagram registration process, should be regarded as the "initial layer" of information about processing provided to the data subject, and further states that the EDPB guidance refers to *"the privacy statement/notice"* as the first layer, and not the registration process. FB-I submits that relevant information on the default purpose of processing can be found in the Data Policy itself, and is also provided in full to the data subject within *"two taps"* – *"(i.e., the Data Policy (first tap), and the Help Centre page (second tap))"*.
- Third, FB-I contends that the GDPR does not require the provision of explicit or specific information on the purposes of processing to data subjects, and states that it would constitute a disproportionate provision of information to data subjects to do so. FB-I submits that the EDPB recognises²⁰² the tension between the form of information provision, and the need to provide the information which is specified in the GDPR.
- Fourth, FB-I contends that the GDPR does not require the Data Policy to include a statement to say that Instagram policies are set to "public" by default.

Conclusion and Finding 1

175. In response to the above issues, although the GDPR does not specify the means by which information must be provided to data subjects, the form and quality of such information is prescribed by the GDPR in Article 12(1) (e.g. concise, transparent, intelligible and easily accessible). FB-I has determined the means by which it provides information (a series of

²⁰¹ Guidelines on transparency under Regulation 2016/679, WP260 rev. 01, paragraphs 6 and 24

²⁰² Ibid. paragraph 34

hyperlinks between online notices containing information). My assessment of Articles 12(1) and 13(1)(c) considers the concrete transparency measures adopted by FB-I in practice. However, my approach to transparency is not predicated on the view that the GDPR requires the provision of certain information in certain layers or formats.

176. FB-I submits that the DPC should give “*due weight to the flexibility afforded to controllers in discharging their transparency obligations as envisaged in the GDPR and by the EDPB*”. While the GDPR affords controllers a degree of flexibility in the way they comply with transparency requirements (e.g. a controller may devise an appropriate system of policies and notices to provide information), nevertheless, the GDPR prescribes mandatory and objective standards of transparency in Articles 12(1) and 13(1)(c), which are not flexible in operation. Controllers are obliged to discharge their transparency obligations in such a manner that ensures compliance with Articles 12(1) and 13(1)(c) GDPR, and I must make an objective decision on the practical measures implemented by a controller in this regard.

177. With regard to the EDPB recommendations regarding the use of layered privacy policies, it is clear that the objective of a layered approach is to resolve the tension between concision and detail. Concepts such as an “initial layer” of indicative information, or navigation within “two taps” are illustrative examples of good design which may facilitate transparency. However, my role is to assess the compliance of FB-I’s actual transparency measures against the standards prescribed by Articles 12 and 13 GDPR, which requires a full assessment of fact. As I have stated in the context of previous Inquiries involving FB-I, an assessment of Article 12(1) in the context of a layered provision of information does not require making deliberations about each individual *layer*, but instead requires an assessment as to whether information has in fact been provided, and whether such provision complied with the form and quality required under Article 12(1). I note that in my above assessment, I have commented on the lack of information during the registration process concerning the purpose of public-by-default settings. However, while I have pointed out the lack of “*just-in-time*” information as part of the registration process (which would have been an obvious contextual setting for such information), I nevertheless agree that the GDPR does not mandate the inclusion of such information at the point of registration.

178. Accordingly, when considering FB-I’s provision of information from the perspective of Articles 12 and 13, I have considered the actual information provided (for the purpose of Article 13(1)(c) GDPR), as well as the form and quality of this information (as required under Article 12(1) GDPR). I note FB-I’s submission²⁰³ that the relevant information was independently provided by both the Data Policy and the associated section of the Help Centre.

²⁰³ FB-I’s submission of 9 August 2021, paragraph 40

179. FB-I contends that it was sufficient for the purposes of Article 12(1) and 13(1)(c) GDPR that the Data Policy stated that the purpose of processing included *“the provision of the Facebook Products (i.e., the Service) to all users”*. I do not accept this contention for the reason that such a statement of purpose would be too general to comply with the GDPR. As is outlined above at paragraph 81, a description of purpose under the GDPR must be sufficiently specific and explicit to enable the proper functioning of data protection law. I do not accept FB-I’s submission in this regard.

180. To the extent that the Data Policy also stated that user information *“can be seen by anyone, on or off our Products, including if they don’t have an account. This includes ... content you share on a ... <public Instagram account.>”*, I am not satisfied that a child user of Instagram would understand from this statement that a default processing purpose applied with regard to the user’s Instagram Account, because this information is phrased in general terms, making no reference to the application of default account settings to Instagram accounts. I am further not satisfied that the hyperlink associated the phrase *“public Instagram account”* in the Data Policy was a sufficient measure for the purpose of Article 12(1) to direct a child user of Instagram to additional information about default settings or private accounts (which are not mentioned in the Data Policy). I do not agree with FB-I’s submission that navigation of the Data Policy was a simple matter of “one tap” in order to find relevant information; the Data Policy is a complex and lengthy description of processing in the context of multiple services offered by FB-I. Navigation of the content of the Data Policy would have involved in-depth consideration, comprehension and analysis by child users as young as 13. FB-I is not correct to assume that all information that can be technically navigated quickly by means of hyperlink (in terms of the number of clicks or taps required) will meet the obligations of Article 12(1) GDPR; the full context of information provision must be taken into account.

181. FB-I submits²⁰⁴ that it is not obliged to provide information about specific or explicit purposes of processing under the GDPR, and suggests that such an interpretation would require a disproportionate provision of information to data subjects. I do not accept this contention in general, because it is clear from the scheme of the GDPR including Article 5(1)(c) (the principle of purpose limitation) and related Recitals (including Recital 39), that the functioning of the GDPR depends on well-defined statements of purpose by controllers. In a more specific sense, it is clear from FB-I’s expression of the purpose²⁰⁵ of public-by-default processing in the Help Centre webpage that this type of information

²⁰⁴ FB-I’s submission of 9 August 2021, paragraph 43

²⁰⁵ *“By default, anyone can see your profile and posts on Instagram. You can make your account private so that only followers you approve can see what you share. If your account is set to private, only your approved followers will see your photos or videos on hashtag or location pages.”* Appendix B to FB-I’s submission of 27 October 2020

can be provided to data subjects in a form that is not disproportionate, and does not lead to information fatigue.

182. FB-I is not correct in its reading of the Transparency Guidelines insofar as it suggests²⁰⁶ that the EDPB has advised against the provision of explicit or specific information on the purpose of processing. FB-I cites paragraph 34 of the Transparency Guidelines, which states:

“There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines [...] how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information”

The key qualifier in the above passage is *“within the legal requirements of the GDPR”*. The EDPB acknowledges the need to resolve the tension between concise information and comprehensive information, but the EDPB does not recommend that a controller can depart from the fundamental requirements of the GDPR, such as the requirement to properly specify the purpose of processing, and to inform the data subject as to the purpose of processing.

183. FB-I contends²⁰⁷ that the GDPR does not require the specific inclusion in the Data Policy of information concerning the fact that it has *“pre-selected a specific processing purpose for sharing Instagram users’ content (public-by-default)”* as referred to above at paragraph 164. FB-I is correct, insofar as the GDPR does not require any specific information to be contained in a privacy policy, nor does the GDPR specifically require the provision of information on user-controlled privacy settings. However, in the circumstances of this case, the public-by-default processing constitutes a discrete purpose of processing, which must be notified to Instagram users to meet the requirements of Article 13(1)(c) GDPR. The above assessment of the Data Policy at paragraph 164 does not assume that FB-I ought to have included any specific information in the Data Policy; rather, in circumstances where FB-I itself contends that the Data Policy is the source of relevant information on the purpose of processing, I have assessed the content of this policy document.

²⁰⁶ FB-I’s submission of 9 August 2021, paragraph 43

²⁰⁷ FB-I’s submission of 9 August 2021, paragraph 44

184. In conclusion, Article 12(1) GDPR expressly recognises that child users may not be aware of the risks and consequences of having a public account by default, and therefore a high standard of transparency is required of FB-I when explaining the public-by-default purpose of processing social media content on Instagram. On balance, I am of the view that the information provided by FB-I concerning the default processing purpose was not provided in a clear or transparent form. In reaching this conclusion, I have taken into account the fact that explicit information on the purpose of the public-by-default processing was limited to certain Help Centre webpages and ancillary materials that required multiple navigation steps on the part of the user (including navigation of the relevant sections of the Data Policy, and the use of hyperlinks which were not worded in a form that would have been clear to a child user). The lack of clear indicative or summary information on this purpose of processing had the effect that the registration process and Data Policy failed to refer child users to more complete sources of information. Accordingly, the form in which information was provided by FB-I was not in compliance with Article 12(1) GDPR.

Finding 1

In circumstances where Facebook Ireland Limited did not provide child users of Instagram with information on the purposes of the public-by-default processing (i.e. operating a social media network which, by default, allows the social media posts of child users to be seen by anyone) in a clear and transparent form, I find that Facebook Ireland Limited has not complied with its obligations under Article 12(1) GDPR.

This finding does not relate to the modified Instagram registration process for child users, which was notified to the DPC by Facebook Ireland Limited in 2021.

Consideration of second transparency obligation

185. I have next considered whether (prior to 4 September 2019) FB-I provided child users with information as required under Articles 12(1), 13(1)(c) and 13(1)(e) GDPR, in connection with the contact information processing.

186. There is no GDPR requirement to provide all information in a specific Data Policy, and it may be appropriate and more effective to provide information to data subjects using a “just-in-time” notice. For the purpose of assessing the information provided by FB-I to child users (prior to September 2019), I have considered the information and option screens shown to users²⁰⁸ during the account switching process, as well as other sources of information provided to data subjects by FB-I.

²⁰⁸ As set out in Appendix J to FB-I’s submission of 27 October 2020

187. With regard to its provision of information to data subjects, FB-I contends²⁰⁹ in its submission of 18 December 2020 that the information provided as part of the switching process was provided in the context of users who had freely decided to switch to a business account, as follows:

"...the introductory screens of the "switching" flow...preview to users the benefits and functionalities of a Business Account and explain that users "Get New Contact Options" and can "Add a contact button to your profile to make it easier for people to get in touch with you." ...the introductory pages of the flow contain an X at the top that allows the User to immediately close out the flow if they are not interested in the functionalities offered with Business Accounts, thereby supporting the fact that any Users that continue to switch to a Business Account, and display contact information as part of that, do so at their own election, in a fully informed manner, and in order to avail themselves of that functionality"

At the same time, FB-I acknowledges that it provided the business account function to all Instagram users, including child users aged 13 or older. As a general issue of transparency under the GDPR, I do not agree with FB-I's presumption that child users who switched accounts were fully informed with regard to the publication of their contact information. In particular, and on the basis of the following detailed analysis of the process, I am not satisfied that the information provided during the switching processing would have alerted child users to the surprising consequences of switching to a business account, which resulted in publication of phone numbers and email addresses provided at the time of registration for a personal account.

188. I have first considered whether FB-I complied with **its obligations under Articles 12(1) and 13(1)(e) GDPR**, to provide information to data subjects describing the recipients of their personal data. In this regard, FB-I contends in its submission of 9 August 2021 that the DPC should give due weight to the entirety of the pre-September 2019 account **switching process**, as well as the **Data Policy** and information provided in the **Instagram Help Center**. FB-I provided the DPC with a copy of the switching process, as Appendix J to its submission of 27 October 2020.

189. The switching process described in Appendix J is titled *"Transition to Business Account - Prior to the changes to Professional Accounts in late summer 2019"*. It appears from the wording²¹⁰ of the switching process that switching to an Instagram business account during this time required a linked profile on the Facebook social media network.

190. It also appears that two different versions of the switching process were used during this time, depending on whether the user was *"Facebook connected"* (i.e. had a Facebook

²⁰⁹ FB-I's submission of 18 December 2020, paragraph 41

²¹⁰ *"Business Profiles on Instagram are linked to Facebook Pages and are subject to their Terms."* Appendix J to FB-I's submission of 27 October 2020, page 3

account linked to their Instagram account) or was "*not Facebook connected*" at the time of switching.

191. The initial five information screens of the switching process were common to both versions of the process:

- Screen 1 was the "*Account*" section of the Instagram settings, which included text stating "*Switch to Business Account*". This text acted as a button to commence the switching process;
- Screen 2 was a generic introductory screen which stated "*Welcome to Instagram Business Tools*";
- Screen 3 described the tools available to business account users of Instagram;
- Screen 4 informed the user that they could create marketing promotions;
- Screen 5 stated "*Get New Contact Options*", and "*Add a contact button to your profile to make it easier for people to get in touch with you*". The wording of the screen did not make clear that the "*new contact options*" were in fact mandatory for business account users. While this statement may have been intended a reference to "*options*" for persons contacting a business account, the language used was not clear, and could reasonably have given rise to an impression in child users that processing of contact information data was optional on the part of the user, and need not be disclosed to further recipients. It is also the case that the term "*People*" used in this information screen did not distinguish between registered users of Instagram, and the world at large.

192. The remainder of the switching process for "*Facebook connected*" users was as follows:

- Screen 6 allowed users to link an existing Facebook profile to their Instagram account, or to create a new Facebook profile. Users were informed that "*Business Profiles on Instagram are connected to a Facebook Page*"; and
- Screen 7 was titled "*Review Your Contact Info*". This page stated "*These contact options will be linked to your business profile. You can edit them any time*". This screen included fields for the user's contact details (email, phone and address). A note at the end of this screen stated "*People will be able to email, call and get directions to your business from new buttons and links on your profile*". This screen did not specify which *people* (i.e. recipients) would have access to the user's contact information, and further, the term "*will be able*" may have been construed by child users as a *conditional* indication on the part of FB-I that an additional contact-publication feature could be implanted by the user (pending some additional steps on the part of the user).

193. The remainder of the switching process for “non Facebook connected” users was as follows:

- Screen 6 included a function which allowed the user to categorise their business account by type. This screen stated “...this will helps [sic] people understand what your business is about”. This statement did not clarify the audience for this category of information.
- Screen 7 was titled “Review Your Contact Info”. This screen included a field for an email address. This screen stated “These contact options will be linked to your business profile. You can edit them anytime [sic]”, and “People will be able to email, call and get directions to your business from new buttons and links on your profile”. This screen did not specify the *people* who would have access to the user’s information, as recipients of personal data, and further, the term “will be able” may have been construed by child users as a *conditional* indication on the part of FB-I that an additional contact-publication feature could be implemented optionally by the user (pending some additional steps on the part of the user).
- Screen 8 was titled “Set Up Your Business Profile”. This screen also contained fields for the user’s email, phone and address. This screen stated “People will be able to email, call and get directions to your business from new buttons and links on your profile”. This screen also included what FB-I refers to as a “toggle” or a switch. This toggle allowed users to change to a public Instagram account from a private account. This *toggle* was accompanied with explanatory text which stated “To switch to a business account, your account must be public”.

194. With regard to Screen 8, FB-I submits²¹¹:

“A lay person’s...interpretation of the word “public” in this context would equate to what the Commission has described as “the world at large”, and if there were any room for doubt in this regard it would have been removed by this information provided in the Data Policy... Additionally, this toggle was located on the same screen through which users could input their email, phone, and/or address details, following a clear statement that: “People will be able to email, call and get directions to your business from new buttons and links on your profile.” Read in context, particularly with all the additional information provided in the switching flow (including another statement that information will be “displayed” and “be public”), this statement further clarifies that “people” – i.e. not just users – would be able to interact with the user going through the switching flow via “new buttons and links” on their Business Account (should they choose to complete that flow).

²¹¹ FB-I’s submission of 9 August 2021, paragraphs 51 and 52

195. I do not agree with FB-I's submission on Screen 8 for the following reasons:

- The concept of a "*public account*" on Instagram exists independently from the specific context of a business account. Public Instagram accounts did not normally include publication of the user's contact information to the world-at-large, unless the account was also a business account. Because of this, a child user may have associated the term "*public account*" on Screen 8 with the characteristics of more typical (i.e. non-business) public accounts, which would have been more familiar to Instagram users. Accordingly, I do not agree that the term "*public account*" in Screen 8 would have been understood by a child user as cognate with publication of contact details which were otherwise normally kept private by FB-I.
- The reference to unspecified "*people*" who would "*be able*" to contact the user using "*new buttons and links*" on the user's profile was not sufficiently clear as an explanation of the recipients of personal data, from the perspective of a child user. In particular, this statement did not specify the categories of persons who would be able to contact the user, and further, the term "*will be able*" may have been construed by child users as a *conditional* indication on the part of FB-I that an additional contact-publication feature could be implanted by the user (pending some additional steps on the part of the user). This statement did not include a concrete indication that FB-I would in fact display the user's contact information to the world at large, in language that would have been clear to child user.
- The relevant section of the Data Policy referred to by FB-I does not define the term "Public information" in a manner that would make clear to a child user that their contact details specifically would be published to the world at large as part of the business account. It is not clear that a child user reading the information provided would have understood this section of the Data Policy to mean that information which is usually kept private for Instagram users would move into the public domain, and be made available to the world at large.
- FB-I is manifestly incorrect to state that the words "*displayed*" and "*be public*" as used in Screen 8 would clarify the recipients of personal data. The term "*displayed*" in Screen 8 was used in reference to "*information you don't want displayed*" (*emphasis added*); this phrase does the precise opposite of what FB-I suggests; it would lead a child user to believe that publication of contact details to the world-at-large was in some way optional or conditional, and not a mandatory aspect of the business account. Equally, the term "*be public*" was used specifically in the context of a public account, and not in relation to the user's contact details. Not all public accounts include publication of contact information; the publication of contact details was limited to business accounts, and accordingly the term "*public account*" could be construed as a reference to accounts which do not involve the publication of contact information. I do not

agree with the contention that a child user may have been informed by these words (in the manner suggested by FB-I) because these words have been taken out of context. While FB-I is entitled to advance a holistic approach to the provision of personal data, the GDPR requires the provision of specific information; it is not sufficient to create a general impression regarding the recipients of personal data.

- It also appears from Appendix J to FB-I's submission of 27 October 2020 that Screen 8 was not provided to users who were already "*Facebook connected*", who were apparently shown a more curtailed version of the switching process.

196. FB-I further contends that certain information provided in the Data Policy would have informed the data subject with regard to recipients of this personal data, to the extent that the Data Policy states:

"Public information can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your public profile on Facebook; and content you share on a Facebook Page, public Instagram account or any other public forum, such as Facebook Marketplace".

197. I do not agree with FB-I's contention in this regard, because it would not be clear to a child user that their contact details, which were obtained by FB-I at the point of registration and not ordinarily published as part of a public or private Instagram profile, would in certain limited contexts be treated as "*public information*" by FB-I. Further to this, the information contained in the **Instagram Help Center** (as furnished to the DPC by FB-I in Appendix B to its submission of 27 October 2020) referred generally to account visibility and audience settings, but did not inform the user that contact details of business accounts would be made public.

198. I have also considered whether FB-I complied with **its obligations under Articles 12(1) and 13(1)(c) GDPR**. In its submission of 9 August 2021, FB-I contends that the Data Policy made the purpose of processing clear, on the basis that a section titled "*Provide, personalize and improve our Products*" indicated that "*the provision of the Service*" is one of the purposes for processing user data. FB-I submits that the DPC cannot accept FB-I's legal basis for processing (as described in Part E above) while at the same time finding that FB-I infringed Article 13(1)(c) of the GDPR. I do not accept FB-I's submission that this information in the Data Policy would serve as an adequate explanation of the purpose of processing, because it is not sufficiently specific for the purposes of the GDPR merely to say that "*service provision*" is the purpose of processing. For the same reason, I do not accept FB-I's contention that a finding of compliance with Article 6(1)(b) GDPR is equivalent to a finding that the purpose of processing is "*service provision*". The assessment of purpose in Article 6(1)(b) is objectively different to the assessment of

purpose in Article 13(1)(c) GDPR; one refers to the objectives of a contract, whereas the other refers to the reasons for processing personal data. I refer to the additional analysis of this issue at paragraph 81 above.

199. In this case, I am of the view that the purpose of obtaining and displaying email and phone numbers of business accounts prior to September 2019 was to create a comprehensive and reliable off-Instagram contact information function for all business profiles, without exception or the ability to opt-out. This purpose was evident from the mandatory requirement of either a phone number and/or email address, and from the mode by which FB-I populated the *“Review Your Contact Info”* form with information it already held, as provided by the user on registration. In a broad sense, it was not inaccurate for FB-I to summarise the purpose of processing as being to *“make it easier”* for *“people”* to contact a business account user, however, this summary of purpose was excessively general (when viewed from the perspective of a child user, who may not appreciate the possible consequences of publishing their phone or email contact information). In particular, this statement of purpose failed to mention that the user’s contact information would be accessible to the world at large (including to persons off-Instagram), and not just to registered Instagram users.

200. Having considered above FB-I’s compliance with Articles 12(1), 13(1)(c) and 13(1)(e) GDPR, I am not satisfied that that FB-I took appropriate measures to provide information to child users on the recipients of personal data and/or the purpose of processing, using clear and plain language. Older Instagram users, or traditional business operators, may have understood the consequences of providing their contact information based on the information provided in the switching process, Data Policy and Help Center. However, the language used by FB-I during the switching process presented the contact information processing in a benign and positive way, and did not describe the purpose of processing, or recipients of personal data in clear language that a child user would fully understand. A child user encountering this information may not have understood the intended category of recipients or the purpose of processing; that the *“people”* referred to meant a global audience of strangers beyond the knowledge or control of FB-I, or that *“making easier”* meant publication of sensitive personal contact details in a way that risked unintended disclosure and loss of control over personal data.

FB-I’s submissions in response to the PDD

201. In its submission of 9 August 2021, FB-I raised additional issues²¹² regarding its compliance with GDPR transparency obligations in relation to the contact information processing, in the following terms.

²¹² FB-I’s submission of 9 August 2021, paragraphs 46 to 61

202. FB-I contends that the DPC (in the PDD) adopted a prescriptive view on the mode by which information should be provided, which focused on the provision of information to data subjects as part of the account switching process²¹³. FB-I submits that *“by focusing on the switching flow without giving proper consideration to the Data Policy and other materials Facebook Ireland provided regarding Business Accounts, in accordance with its GDPR transparency obligations and the flexibility it is afforded in this regard, the Commission’s assessment is also too narrow”*.

203. Without prejudice to FB-I’s previous submissions to the DPC (which sought to rely primarily on the account switching process as the source of relevant information) FB-I now contends that the necessary information was otherwise made available to child users *“holistically”* by information provided in the switching flow, the Data Policy, Terms of Use, and other Help Centre materials.

204. I accept that FB-I is entitled to provide information to data subjects in more than one document, subject to the substantive requirements of Articles 12(1) and 13 GDPR. Equally, FB-I is entitled to rely on the full suite of documents provided to data subjects as a means of complying with its transparency obligations; however, in the context of the PDD, the emphasis on the switching process as a means of providing information to data subjects was directly reflective of FB-I’s submissions. Indeed, in its submission of 18 December 2020, FB-I stated:

“Facebook Ireland did not intend for the Terms of Use or the Data Policy to go into such a level of granular detail, [concerning the display of contact details on business account profiles] but rather has taken the approach that it would be more effective to provide the appropriate information “just-in-time” (i.e., at the point when Users are considering switching to a Business Account).”

It was open to FB-I, at all times since the commencement of this Inquiry, to advance a *holistic* approach to transparency, but FB-I instead chose to focus on the switching process as the mode of information provision. It is therefore difficult to accept FB-I’s criticism in this regard.

205. FB-I also contends that the primary basis for the DPC’s adverse views on FB-I’s compliance with Article 12(1) with regard to the contact information processing is the *“absence of information specifically in the switching flow disclosing perceived risks associated with allowing information to be made public”*. In support of this position, FB-I cites paragraph 200 above (which refers to “unintended disclosure and loss of control” to “strangers” as a class of potential recipients of personal data), as well the reference at Paragraph 160 above to Recital 39 GDPR. FB-I submits that the provision of information to data subjects on perceived risks is not a requirement of the GDPR, and further states

²¹³ Appendix J to FB-I’s submission of 27 October 2020

that Recital 39 does not act as an operative provision of the GDPR to create such a provision. I do not accept FB-I's summary of the DPC position in this regard; the primary basis for my adverse finding concerning the contact information processing is based on FB-I's failure to take appropriate measures required by Article 12(1) GDPR in relation to information required under Articles 13(1)(c) and 13(1)(e) GDPR. This finding is a direct application of the operative provisions of the GDPR, and is not based on the application of a Recital. Recital 39 is nevertheless relevant in this context insofar that it specifies the mode of provision of information on the purpose of processing, as follows: "*...the specific purposes for which personal data are processed should be explicit and legitimate*". Reading Article 12(1) in light of this Recital, it is clear that the GDPR requires controllers to provide information (on the specific and explicit purposes of processing) in a form that is intelligible to a child. Accordingly, my findings are not predicated on the view that FB-I ought to have specifically informed child users as to specific **risks** arising from contact information processing; the basis of the finding is that FB-I failed to provide the specific information to child users (as required in Articles 13(1)(c) and/or (e) GDPR) in the form required by Article 12(1) GDPR.

206. FB-I contends that the Transparency Guidelines do not require the provision of information on risk. In this regard, FB-I acknowledges the recommendation that, in addition to the information contained in Articles 13 and 14, "*controllers should also separately spell out in unambiguous language what the most important consequences of the processing will be*"²¹⁴. FB-I contends that the Transparency Guidelines expressly limit this transparency obligation to "*complex, technical or unexpected data processing*", and also allow for flexibility on the part of controllers, insofar that the guidelines state: "*data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects*". FB-I states that it conducted an assessment of risk, and concluded that: "*(a) the processing was not of a type such as to warrant 'spelling out' specific consequences of such processing, at least not in the manner suggested by the Commission in the PDD; and (b) the potential manifestation of such risks was sufficiently mitigated by the measures and safeguards it has put in place*".

207. While I do not agree with FB-I's contention that the contact information processing was not complex or unexpected, FB-I's submission is not relevant to the issue at hand, which concerns the application of Article 12 and 13, and not the wider GDPR obligations described by the Transparency Guidelines.

208. In conclusion, FB-I contends that its compliance with transparency obligations in relation to the contact information processing must be assessed holistically, taking into account the switching process, the Data Policy and relevant Help Centre articles explaining what it meant to have a public account. FB-I submits that users sought out the business

²¹⁴ Guidelines on transparency under Regulation 2016/679, WP260 rev. 01, paragraph 10

account function deliberately, and would have understood that their contact information would be public. In response, I have considered all of the documents identified by FB-I as the source of relevant information on processing, and I have considered the controller's submission that all of these documents contributed to its compliance with Articles 13(1)(c) and 13(1)(e) GDPR. Having conducted a holistic assessment of the information provided, I am not satisfied that FB-I provided this information using clear and plain language that a child user could understand.

Conclusion and Finding 2

209. Bearing in mind the requirement of Article 12(1) GDPR that controllers must take appropriate measures to provide information using clear and plain language, in particular when addressed to a child, and taking into account the interpretative approach described in Recitals 38 and 39 GDPR, I am satisfied that the information provided to child users by FB-I in respect of the contact information processing (prior to 4 September 2019) was not in compliance with Article 12(1) GDPR. In particular, the language used when providing information to child users did not make clear the purposes of processing (as required under Article 13(1)(c) GDPR) or the categories of recipients of personal data (as required under Article 13(1)(e) GDPR) in clear or plain language, when viewed from the perspective of younger child users of Instagram.

Finding 2

In circumstances where, prior to 4 September 2019, and in connection with the processing of email addresses and/or phone numbers of Instagram business account profiles, Facebook Ireland Limited did not take measures to provide child users with information on the purposes of processing and/or information on the categories of recipients of personal data (as required under Articles 13(1)(c) and (e) GDPR) using **clear and plain language**, I find that Facebook Ireland Limited has not complied with its obligations under Article 12(1) GDPR.

Consideration of third transparency obligation

210. I have next considered whether, after 4 September 2019, FB-I provided child users with information as required under Articles 12(1), 13(1)(c) and 13(1)(e) GDPR, in connection with the contact information processing.

211. The Facebook Data Policy states generally that “*any information you share with a public audience*” will be public, but does not specifically refer to the optional facility to publish a phone number or email address in the context of a business account. Information provided to users on switching to a business account was primarily contained in the account switching process.

212. As noted above, it is not required that the Data Policy (as a standalone document) must provide the full extent of information on processing. For the purpose of assessing the information provided by FB-I to child users (after 4 September 2019) on the processing of contact information, I have considered the information and option screens shown to users²¹⁵ during the account switching process, as relied on by FB-I as the relevant source of information. In the course of switching account, users were shown a preliminary information screen which stated “[a]dd a contact button to your profile to make it easier for people to get in touch with you”. This information notice was followed by an option screen relating to the use of contact information, titled “Review Your Contact Info”. This option screen included fields for email and phone contact information, and stated “This information will be displayed on your profile publicly so people can contact you. You can edit or remove this information at any time”. The option screen also included an opt-out button at the end of the screen, which stated “Don’t use my contact info”.

213. FB-I was obliged to provide data subjects with information on the purposes of processing, as well as information on the categories of recipients of personal data. Since September 2019, FB-I has changed the wording of the “Review Your Contact Info” screen to inform users that their contact details will be “displayed...publicly”, where in the past the same screen omitted any express reference to the public display of information.

Conclusion and Finding 3

214. Bearing in mind the requirement of Article 12(1) GDPR that information addressed to a child must be provided using clear and plain language, and taking into account the interpretative approach described in Recitals 38 and 39 to the GDPR, I am satisfied that the information provided to child users by FB-I (after 4 September 2019) in the course of the business account switching process was in compliance with Articles 12(1), 13(1)(c) and 13(1)(e) GDPR.

Finding 3

I find that, as of the date of commencement of this Inquiry, the information provided to child users by Facebook Ireland Limited in relation to the processing of email addresses and/or phone numbers of Instagram business account profiles was in compliance with Article 12(1), 13(1)(c) and 13(1)(e) GDPR.

Consideration of fourth transparency obligation

215. I have next considered whether FB-I adequately notified existing business account users of the removal (on 4 September 2019) of the requirement to publish a phone number and/or an email address in the context of a business account. In this regard, I have

²¹⁵ As set out in figures 6 and 7 above, taken from Appendix I to FB-I’s submission of 27 October 2020

considered whether FB-I's processing in this regard was fair and transparent for the purposes of Article 5(1)(a) GDPR.

216. On 4 September 2019, FB-I modified the purpose of processing contact details of Instagram business profiles. In particular, the purpose of processing changed from the purpose of publishing off-Instagram contact information for all business accounts, to the narrower purpose of facilitating publication of off-Instagram contact information where the user opted to make this information publicly available.

217. Article 13 GDPR requires the provision of information to data subjects *"at the time when personal data are obtained"*. The Transparency Guidelines²¹⁶ adopt the following recommendation with regard to information updates:

"The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14...However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing)"

218. FB-I modified its processing operations on 4 September 2019. Users who registered after this time were provided with information on how to opt-out of the provision of contact information. FB-I modified its Instagram Help Centre webpage regarding business accounts on 18 October 2019, and subsequently published a blog post entitled *"New and Updated Tools for Businesses"* on 20 December 2019²¹⁷. Although FB-I submits generally that it *"utilises dynamic in-product notifications and tips to highlight new tools or features available to Users, including Teens"*, FB-I does not appear to have used such methods to inform existing business account users that public contact information could be removed from the user's profile. It also appears that the static sources of information provided in

²¹⁶ WP260 rev.01, page 17

²¹⁷ <https://business.instagram.com/blog/new-and-updated-tools-for-businesses>

the form of Help Centre webpages and the blog were provided a number of weeks after the change in processing was implemented. It further appears from FB-I's submission that it was aware, prior to 4 September 2019, that certain business account users did not want to publish their email and phone information, as is clear from FB-I's statement²¹⁸ that prior to the September 2019 changes:

"Some businesses...noted that they preferred to have flexibility in providing additional contact information on their profile and, indeed, preferred to communicate with their audience or customers through direct messaging on Instagram rather than traditional means (like phone or email)."

219. Despite being aware that some existing business account users were apparently reluctant to publish their contact information, FB-I did not immediately notify these users of the change in processing purposes, and did not implement any direct notification method when providing information on changes to the business account.

FB-I's submissions in response to the PDD

220. In its submission of 9 August 2021, FB-I made the following submissions²¹⁹ in relation to this issues.

221. FB-I contends that the three elements stipulated in Article 5(1)(a) GDPR for personal data to be processed "*lawfully, fairly and in a transparent manner*" should be regarded as a cumulative legislative requirement. FB-I contends that as a result of this cumulative construction "*in order for there to be a contravention of Article 5(1)(a) then the process [sic] must be unlawful, unfair, and non-transparent*". I do not accept FB-I's proposed construction of Article 5(1)(a) GDPR. The legislative intent of Article 5(1)(a) GDPR is clear; it places an obligation on controllers to ensure that processing meets three distinct criteria, all of which are independently required on the part of a controller. FB-I's approach suggests that Article 5(1)(a) creates a single, cumulative obligation, with three constituent elements. Even if FB-I is correct in this regard, a lack of transparency alone would mean that the *cumulative* requirement had not been met. The cumulative requirement obviously applies to the controller, and not the DPC. I am satisfied that a failure to comply with any one of the conditions described in Article 5(1)(a) would be contrary to the GDPR, and sufficient to ground a finding of an infringement by the DPC. Accordingly, it would be sufficient in the context of Finding 4 to find that the processing was either not fair, or not transparent.

222. FB-I contends that the PDD has not shown sufficient evidence of unfairness to ground a finding under Article 5(1)(a) GDPR. FB-I submits that the DPC approach:

²¹⁸ FB-I's submission of 27 October 2020

²¹⁹ FB-I's submission of 9 August 2021, paragraphs 62 to 67

“...appears to be tied to the manner in which transparency about a product functionality change was provided to certain data subjects. This is because Facebook Ireland did provide resources to [Child Users] after its Business Account product functionality changed in a form that no longer required contact information – it would appear just not the kind of resources that the Commission would have wanted Facebook Ireland to provide. It is one thing if Facebook Ireland had provided no information to its users about the change in the requirement to provide contact information with Business Accounts, however Facebook Ireland did provide Help Centre resources and a blog post that provided information accessible to all data subjects. Facebook Ireland submits that what amounts to a divergence of views as to what form to provide the transparency should not be the basis of a finding of infringement of this nature.”

I do not accept FB-I’s submission in this regard, which has misconstrued the DPC position. As is set out above, there was a period of time after the implementation of the revised switching process where no relevant information was provided to inform child users that the obligation to process contact information had been removed (unless, as is unlikely, a child user switched to a personal account, and then switched back to a business account during this time). Further to this, I do not accept FB-I’s contention that the form of transparency is immaterial. As the Transparency Guidelines state in relation to updating data subjects to changes, “...the method used to bring the changes to the data subject’s attention should be explicit and effective...This is to ensure the data subject does not “miss” the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDR”. In particular, the use of passive information resources (as used by FB-I in this case) as the mode of informing existing business account users about changes poses the risk that the update will not be noticed (at least without some dynamic indication to users that something has changed). It would not be fair or transparent to expect users to monitor the full suite of information resources provided by FB-I in order to identify relevant changes to processing. Therefore, taking into account the initial delay on the part of FB-I in updating its information, and the eventual form of that update, I am of the view that FB-I was not in compliance with Article 5(1)(a) GDPR.

223. FB-I submits that it is contradictory for the DPC to find an infringement of the GDPR in respect of measures which are also cited as mitigating factors, as follows:

“Facebook Ireland also submits that the Commission’s reasoning supporting its finding of infringement is inconsistent. While the Commission, on the one hand, determines that Facebook Ireland’s processing was “unfair” because, in its view, the transparency to users was ineffective, it on the other hand, considers that the Instagram Help Centre and blog post regarding the change it implemented in

September 2019 to cease requiring Business Accounts to publicly display at least one contact detail was **“mitigating in respect of FB-I’s infringement of Article 5(1)(a)”** GDPR because it **“[l]ikely made some of the data subjects aware of FB-I’s removal of the requirement.”** Facebook Ireland submits that it is contradictory to find that the transparency it provided could be effective in mitigation, yet also constitute an infringement of Article 5(1)(a) GDPR resulting in a proposed significant range of fines.”

224. The above submission by FB-I quotes selectively from the PDD, and neglects to include the very clear explanatory information which accompanied this statement²²⁰, as follows:

*“While, **these static sources of information were not sufficient for the purposes of Article 5(1)(a)** and were provided a number of weeks after the change in processing was implemented, I consider that this action mitigated the damage suffered by some of the data subjects. This action likely made some of the data subjects aware of FB-I’s removal of the requirement and, thus, mitigated the loss of control suffered by those data subjects. I provisionally find that this action is mitigating in respect of FB-I’s infringement of Article 5(1)(a).”*

225. FB-I is incorrect to conflate the concept of *mitigation of damage* referred to in Article 83 GDPR, with the concept of effective GDPR compliance with Article 5(1)(a) GDPR. The term *mitigate* means to make something less severe; it does not have the connotation that a required standard has been met. As was already made clear to FB-I in the PDD, the DPC is of the view that the standard set by Article 5(1)(a) GDPR was not met, but the damage caused to data subjects was nevertheless mitigated to an extent by the (otherwise inadequate) measures implemented by the controller. Accordingly, I do not accept the controller’s view that the DPC approach is contradictory.

226. With regard to its previous statements regarding the introduction of an opt-out for contact information processing, FB-I states:

“...In its prior submission, [FB-I] stated only that “some businesses ... noted that they preferred to have flexibility in providing additional contact information.” A preference is not the same as “reluctance,” and Facebook Ireland respectfully requests that the Commission should amend its finding in this regard.”

Whether the inclination of business account holders to publish their contact details can best be described as a “reluctance” or a “preference” is of little probity to this issue. What is relevant here is the fact, as acknowledged by FB-I, that certain users of business accounts indicated to the controller that they wanted an alternative to the mandatory publication of their contact information. On implementing this

²²⁰ PDD, paragraph 346

suggestion by its users, FB-I did not notify existing business account holders of this amendment in a timely manner, or in an effective form.

227. FB-I also contends that the DPC should take into account “...the transparency provided to Teens who opted to create Business Accounts prior to 4 September 2019 that their business contact information would be public”. FB-I submits that the “fairness of the actions taken by [FB-I] post-4 September 2019 should be assessed in light of the fact that users who shared business contact information via Business Accounts created before that date did so voluntarily and based on the provision of appropriate information”. In this regard, it appears that FB-I is not suggesting that such users were made aware of impending or possible changes to the functionality of business accounts, but rather, FB-I is suggesting that the initial processing arrangement (i.e. default publication of contact information of child users) was sufficiently fair and transparent for the purpose of Article 5(1)(a) GDPR. I do not agree with FB-I’s assessment of the transparency measures adopted in this regard, for the reasons set out in respect of Finding 2; for this reason alone I do not accept FB-I’s submission. In a more general sense, questions of fairness and transparency will vary depending on the context; a significant modification to processing (such as the inclusion of an opt-out for the first time where processing was previously mandatory) would have a consequential impact on what is considered fair or transparent processing for persons affected by the change.

Conclusion and Finding 4

228. I note that although the Help Centre and blog post were (after a delay) made accessible to users, existing business account users (and in particular child users) may not have noticed the provision of this information, in the absence of an appropriate prompt by the controller. I also note that FB-I had at its disposal the technical means to notify existing business account users of the change prior to September 2019, but did not do so.

Finding 4

I find that Facebook Ireland Limited did not adequately inform those child users who switched to a business account prior to 4 September 2019 of the removal (after 4 September 2019) of the requirement to publish their contact information on Instagram business profiles.

Accordingly, I find that processing by Facebook Ireland Limited of contact information of child users who switched to a business account prior to 4 September 2019 was not fair or transparent, contrary to Article 5(1)(a) GDPR.

G. Assessment of certain matters concerning Articles 24, 25 and 35 GDPR

G.1 Nature, scope, context and purpose of the processing

229. This Decision assesses FB-I's compliance with Articles 24, 25 and 35 GDPR with regard to the processing described in Part C.3 above. Articles 24, 25 and 35 GDPR expressly require taking into account the "*nature, scope, context and purposes*" of processing. I have therefore considered each of these four criteria on a preliminary basis, in order to inform the subsequent analysis of the above three provisions of the GDPR in the Draft Decision.

Nature of processing

230. The **nature** of processing refers to the basic or inherent features of the operations performed on personal data by a controller. This Decision relates to two types of processing by FB-I: processing of contact information of child users, and public-by-default processing of social media content of child users. The nature of the processing in question is described in Part C.3 of this Decision.

Scope of processing

231. The **scope** of processing refers to the extent of operations performed on personal data by FB-I. Initially, FB-I informed the DPC²²¹ that there are [REDACTED] child monthly average users of Instagram in the "European Region". In a cover letter to its submission of 9 August 2021, FB-I informed the DPC that it had provided the wrong information in its earlier submission, due to an oversight, as follows:

"...the PDD refers to there being [REDACTED] child users of Instagram in the European Region." Facebook Ireland would like to clarify this number. First, as mentioned in Facebook Ireland's submission to the Commission of 29 October 2020 in Inquiry 20-7-3, this figure refers to the monthly average number of Teen Users of Instagram in the European Region (i.e. the number of users who accessed the service within 30 days). Second, this figure should have read that Instagram has [REDACTED] monthly average Teen Users in the European Region. In providing this number previously, due to an oversight Facebook Ireland only provided figures for users of personal accounts, and is now providing an updated figure to include users of Business accounts ([REDACTED]) and Creator accounts ([REDACTED]) as of that date. Facebook Ireland shall write to your office separately to correct this figure for the purposes of Inquiry

It therefore appears that there are over [REDACTED] child users in the European Region who operate business accounts ([REDACTED] of all Instagram accounts operated by child users have opted to switch to a business account).

²²¹ As per paragraph 22.1 of FB-I's submission to the DPC of 29 October 2020 in separate Inquiry 20-7-3

232. With regard to the contact information processing, the Facebook Data Policy states that public information on Instagram can be seen by “*anyone, on or off*” Instagram. FB-I has, at certain times, made the contact information of child users accessible publically on the web browser version of business account profiles. Prior to September 2019, FB-I required the publication of either a phone number or email address of child users who switched to a business account. FB-I continues to provide a facility whereby child users may publish their personal contact information in the context of an Instagram business account. FB-I has included (as plain text) the contact information of child users in the HTML source code of profile webpages (in the context of business accounts). It is therefore clear that the scope of processing of contact information of child users is very extensive, to the extent that it involved the global publication of information of child users to an indefinite and unrestricted audience, not limited to other users of Instagram.

233. With regard to the scope of the public-by-default processing, by setting accounts of newly registered users of Instagram to “public” by default (unless the user subsequently intervened to switch their account to “private”), FB-I determined that social media posts and content of child users would be shown to a global audience of millions of other Instagram users, as well as other persons off-Instagram. Accordingly, by setting accounts to “public” by default, FB-I determined that the scope of processing of social media content in respect of child users was potentially very extensive, being made accessible without restriction to an indeterminate global audience.

Context of processing

234. The **context** of processing refers to the circumstances that form the setting of the processing. Paragraphs 235 to 255 below set out the context in which FB-I processes the contact information of child users, and has made the content posted by child users on Instagram visible publicly by default.

235. This Inquiry relates to registered Instagram users who are at least 13 years old, and younger than 18 years old (i.e. child users of Instagram). The GDPR recognises children as a vulnerable category of people, and in particular, Recital 38 GDPR notes that children “*merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*”.

236. Phone numbers and email addresses are persistent forms of personal data, which are infrequently changed or abandoned by the holder. These modes of communication can provide direct personal access to child users, without a reliable way of identifying the person making contact. Phone numbers and email addresses can be targeted for fraud and impersonation. These contact details are frequently used as personal identifiers in the context of numerous online services, posing a potential fraud risk. A traditional business or professional may routinely decide to publish their phone or email address as

an essential means of communication with customers, but in general, this type of information is sensitive and would be known only by a person's friends, family, or colleagues. In its submission of 9 August 2021, FB-I observes²²² that "*phone numbers have traditionally been published in a public phone book*". In my view, there are essential differences between traditional residential land-lines, and personal mobile phones. In particular,

- mobile phones are typically personal to one individual, and not shared by a household;
- mobile phone numbers are not typically published in phone books;
- mobile phones allow for direct personal contact at any place or time;
- mobile phone numbers may be used as identifiers for other over-the-top communication services;
- communication by mobile phone would be less obvious to a child's parent or guardian than communication by means of a traditional land-line; and
- public phone books are typically published on a local basis, and would be less accessible than publication of information in an Instagram profile page.

I am therefore satisfied that the publication of traditional land-line numbers in phone books is not a comparable practice to the publication of children's mobile phone and email contact information.

237. Prior to March 2019, and again for a period after August 2020, FB-I included plain-text phone numbers and email addresses in the HTML source code for Instagram business account profile pages. Information in HTML can be collected in bulk by unauthorised third-parties (referred to as "web scraping"). The potential for web scraping of contact information was demonstrated by Mr Stier's engagement with the Facebook Bug Bounty programme, where Mr Stier purports to have obtained contact details of numerous EU-based data subjects via the HTML source code. Phone numbers and email addresses can be collected using web scraping techniques, resulting in loss of control over this personal data, and possible negative impacts for child users. It is also the case that by making contact information of child users public, FB-I could no longer control who had sight of the information, or how it was used.

238. FB-I does not apply age restrictions on who may switch to a business account. The switching process was streamlined and could be completed in a matter of seconds by navigating a series of information and option screens²²³, without the need to input any

²²² FB-I's submission of 9 August 2021, paragraph 76(a)

²²³ FB-I's submission of 27 October 2020, Appendices I and J

text. As part of the account switching process for business accounts, FB-I automatically populated certain information fields with child users' contact information obtained during the "personal account" registration process. In this way, the information which FB-I used to populate the account switching process took information from a personal context, and repurposed it in a professional setting. FB-I relied solely on the decisions of child users as young as 13 when publishing personal contact information, and did not require parental approval to any extent for this processing.

239. The publication of contact information was a mandatory requirement of business account users, until an opt-out was introduced by FB-I in September 2019. FB-I further states that the business account was *"was a product of its time"*, in that it was *"...created in 2016 as a means of allowing more "traditional" businesses the opportunity to better connect their Instagram profile with their "off-Instagram" presence"*. In July 2019, FB-I split the business account feature into two distinct types of professional accounts: *"business accounts"* intended for traditional businesses, and *"creator accounts"* intended for *"activists, artists, bloggers, influencers"*. Child users may use either type of account without limitation. Persons switching to a business account are prompted to publish their contact information (subject to an opt-out). Persons switching to a creator account are not prompted to publish their email or phone contact information.

240. With regard to the processing of contact information of child users, FB-I submits that child users between the ages of 13 and 17 freely decided to publish their contact information in the specific context of professional activities such as entrepreneurship or advocacy. FB-I contends further²²⁴:

"The tools associated with Instagram's Business Account help these kinds of users increase their following and presence on Instagram, and, ultimately, more effectively exercise their rights of free expression and assist them in fulfilling their entrepreneurial and social movement goals. Instagram believes these opportunities should be afforded to all users, regardless of age"

241. FB-I submits²²⁵, that there was no material difference between a business account and a personal account, and further states that both types of account were used in the context of a safe environment, as follows:

"...a Business Account is not materially different in terms of its profile and visibility than any public personal account. As set out in the introduction above, the profile associated with a Business Account looks and feels very similar to a public personal account profile. Both kinds of accounts (Business and personal) share the same general profile design – a profile photo, "free-text" space, followed by the quintessential profile grid, where the account posts pictures or videos appearing in a

²²⁴ FB-I's submission to the DPC of 27 September 2020, paragraph 13

²²⁵ FB-I's submission of 27 October 2020, paragraph 64

row of three squares (see Figure 1 above). As discussed in response to Query 3, Teens operate any kind of account (personal account or Business Account) within the safety-focused environment provided to all users.”

242. This submission by FB-I is not correct. A business account is manifestly different to a personal account in terms of the user’s visibility, because business accounts required/facilitated the publication of personal contact information of child users who switched to business accounts. This publication of contact information (which is specifically built into the account switching process using automatically completed “structured fields”) resulted in the dissemination of information to a wider public context, where neither FB-I nor the child user could control who had access to the information, or how the information might be used. This resulted in information leaving the purportedly “safety-focused environment” of Instagram, and moving to the less-safe context of the world-at-large. Information published in this way has at certain times been published on the web-browser version of Instagram, which posed a risk of web-scraping and permanent loss of control over personal data. Accordingly, while I accept that personal accounts and business accounts are superficially similar in terms of design, there were obvious material differences between these types of account in terms of the information which was published, and the types of safeguards which were required to protect the rights of child users. I am therefore satisfied that FB-I’s submission is without merit in this regard.

243. In contextualising the use of business accounts by child users, FB-I referred the DPC to examples of individuals under the age of 18 who use Instagram in connection with advocacy or commercial purposes, as follows²²⁶:

“Professional Accounts (including Business Accounts) are intentionally made available not just to traditional businesses but to all Users who are – or wish to explore – using Instagram to turn their passion or craft into a possible means for making a living, or in pursuit of other professional opportunities and social or charitable causes. As such, Business Accounts are not solely suitable - or designed - for the purpose of promoting a traditional business. Indeed, not limiting the use of Professional Accounts in this way is important in order to support and enable the innovative ways in which Users are creating professional opportunities for themselves and others through the Service.

For similar reasons, Professional Accounts (including Business Accounts) are not restricted by age -- all Instagram Users (adults and Teens) can utilise the Service in pursuit of a broad array of professional opportunities. Indeed, in the First Submission, Facebook Ireland provided the Commission with numerous press stories where Teens, in particular, have utilised Instagram to transform a new idea or craft into a

²²⁶ FB-I’s submission of 18 December 2020, paragraphs 37 and 38

successful business or other professional endeavour, or have turned their interests or passions into social, political or charitable initiatives. This is something which Facebook Ireland believes it is important to continue to facilitate.”

244. One of the “press stories” specifically referenced by FB-I²²⁷ in this context refers to a “10-year-old” Instagram user (based outside of the European Region) who advertised her business on Instagram, in apparent contravention of the Terms of Use, and without being detected as a person under the age of 13.

245. FB-I submits that the Instagram platform has been designed to be used safely by all people over the age of 13, and provides examples of the safety, information and security features it has adopted in this regard, which are targeted at younger users and their parents²²⁸.

246. Instagram provides a direct message function to facilitate on-platform communication between users. FB-I acknowledges that publication of phone and email contact information was not always preferred from the perspective of business account users, for the following reasons²²⁹:

“Some businesses also noted that they preferred to have flexibility whether to provide additional contact information on their profile and, indeed, preferred to communicate with their audience or customers through direct messaging on Instagram rather than traditional means (like phone or email).”

247. FB-I nevertheless submits²³⁰ that the contact information processing was

“...necessary to provide a service that gives effect to Teens’ fundamental rights to conduct a business, to express themselves, communicate, and engage with information and communicate relevant to their interests and passions, while building community and their own brands.

248. I note FB-I’s statement that child users are “significantly more technically literate than they were a generation ago”²³¹. However, the technical literacy of child users can also increase the likelihood that a child will access professional features that are not intended for use in a personal capacity. In this regard, I note that FB-I offers data analytics tools to business account users (“insights”) including information on how many times a user’s content was shown to other users, and information on the ages and locations of followers. It is very likely that this information would also be of interest to technically

²²⁷ <https://www.thestartupsquad.com/5-girlpreneurs-who-are-crushing-it-on-instagram/> - cited in FB-I’s submission to the DPC of 27 October 2020

²²⁸ Including the features described at paragraph 5 of FB-I’s submission of 27 October 2020

²²⁹ FB-I’s submission of 27 October 2020, footnote 16

²³⁰ FB-I’s submission of 27 October 2020, paragraph 67

²³¹ “Legitimate Interests Assessment (‘LIA’) Processing minors’ data for the provision of the Facebook Products”, 28 January 2021, section 4.2.b

literate child users, and that the existence of this free, otherwise hidden feature would quickly become known to groups of children. The additional information provided (without charge) to business account users on Instagram would incentivise account switching by child users, even if the child user had no intended professional purposes for their account. I also note, in line with Recital 38 GDPR, that child users may not fully appreciate the risks associated with publication of personal contact information to the world at large (as was required prior to September 2019, and is still possible under the revised business account switching process).

249. The context in which the contact information of child users was processed by FB-I therefore relates to certain commercial and professional activities of child users, but also involves circumstances where there was no restriction on who could switch to a business account. Business accounts provided additional functionality without charge, which may incentivised child users to switch accounts even where they did not have a professional purpose in mind for their account. Finally, publication of contact information in the context of a business account could result in the loss of control over sensitive personal data of child users, including publication of information to persons who are not known to FB-I or the user.

250. In terms of the context in which accounts of child users are set to “public” by default on registration, FB-I submits²³²:

“Facebook Ireland confirms that all new Instagram accounts (including Teen accounts) are defaulted to “public” personal accounts, meaning that the account’s audience (i.e., who can see their posts and stories) is not limited to approved followers. People choose to use Instagram as a platform where they can openly share with a diverse, global community, discover new content, and explore shared interests. Because sharing and maintaining an open exchange with the community of other users is at the heart of Instagram, setting profiles to public per default – including those of Teens – is appropriate and fully in line with user expectations. Users expect to seek, discover, and connect with previously unknown content and communities on Instagram, and the user experience would be hampered for new users – who, by necessity, are still developing connections on Instagram – if their ability to participate would be restricted by default. Default public settings are not only appropriate given the nature of the Instagram Service, which people join in order to use, but also because Facebook Ireland designed Instagram to be safe with Teens specifically in mind. From the moment Teens join Instagram, they enter an environment with strong policies and safeguards in place aimed at providing a safe place to facilitate sharing and expression.

²³² FB-I’s submission of 27 October 2020, paragraph 39

251. It is a common expectation²³³ of social media users that they will have control over who sees their content. For example, a 2020 survey conducted by the Commission Nationale de l'Informatique et des Libertés found that 66% of children aged 10-14 and 69% of children aged 15-17 who had at least one social media account had opted to set the account to "private". In its submission of 9 August 2021, FB-I contends²³⁴ that this survey was not specific to Instagram. I note that although the survey covered a number of different social media services, Instagram users featured prominently in the respondents to the survey. FB-I also states that this survey was inapplicable because it was not conducted on a statistically significant test population, and was geographically limited to users in France. The survey involved more than 500 children; it is notable that FB-I considers this number of participants to be insignificant, and yet elsewhere in its submission, FB-I itself seeks to rely on a study²³⁵ which involved 25 participants. I am satisfied that it is appropriate that I should have regard to this survey, as an indication of the clear expectations of child users in an EU Member State with regard to private social media audience settings.

252. This well-established expectation of audience control is also reflected in FB-I's decision to implement the "private" setting for Instagram personal accounts. It is very clear that although many Instagram users have adopted the platform as a place to "*openly share*" content, another cohort of users prefers to limit the sharing of their posts to a controlled audience of followers. It is not clear that Instagram users can be regarded as having a singular expectation that their content will be made public by default. The expectations of users will vary from the outset depending on how they want to use the service, and may change over time.

253. In its submission of 9 August 2021, FB-I further contends that "*public sharing settings can, in many situations, actually improve users' support networks*". In this regard, FB-I cites a survey²³⁶ of 25 transgender adolescents between the ages of 15 and 18, and a research review from 2017²³⁷. Both of these academic sources also acknowledge the possibility of harassment, cyberbullying, depression, social anxiety, exposure to developmentally inappropriate content, and exposure to exclusionary behaviour which are associated with social media use by children. The DPC therefore acknowledges that there are potential benefits and disadvantages to social media user by children.

254. Insofar as FB-I associates the public-by-default processing with access to the benefits of social media use generally, this appears to be a false dilemma; there appears to be no

²³³ See presentation "[Les comportements digitaux des enfants](#)", page 24.

²³⁴ FB-I's submission of 27 October 2020, Annex A

²³⁵ FB-I's submission of 9 August 2021, footnote 152

²³⁶ Selkie, Adkins, Masters, Bajpal, and Shumer, "Transgender Adolescents' Uses of Social Media for Social Support", *Journal of Adolescent Health*, Vol. 66, Issue 3 (2020)

²³⁷ Yalda T. Uhls, Nicole B. Ellison, Kaveri Subrahmanyam, "Benefits and Costs of Social Media in Adolescence," *Pediatrics* Nov 2017

technical reason to apply either public or private audience settings by default at the time of user registration. The public-by-default setting was a deliberate choice on the part of FB-I, intended to maximise user engagement and sharing on the Instagram platform by nudging new users towards a public account. It is not clear how it would “*hamper*” the experience of new users to implement restricted audience settings, or to provide an audience setting choice at time of registration. It is possible to “*seek, discover and connect*” on Instagram without also producing content for wider public consumption. Users with private accounts are not limited in what they can see on the platform. The existence of a person’s account (whether public or private) is public information. Private accounts can also be found using the Instagram search function, thereby facilitating easy connection with other followers. Accordingly, in circumstances where private account users could also engage freely with other users and view content on Instagram, I am not satisfied that the public-by-default processing was intrinsically linked to, or otherwise an essential part of, a user’s enjoyment of the potential benefits of Instagram.

255. Content shared publicly on Instagram is not limited to “*communities on Instagram*”. Such content is also made available (on the web browser version of a profile page) to an indeterminate global audience of persons who are not registered Instagram users. Certain content on the web browser version of Instagram can be seen by anyone without logging in as a registered member²³⁸.

Purposes of processing

256. The **purpose** of processing refers to the reasons for processing personal data. In its submission of 9 August 2021, FB-I contends that the purpose of both types of processing was the provision of the Instagram Service. I do not accept this submission, for the reasons which are outlined at paragraph 81 above.

257. With regard to the processing of contact information prior to September 2019, the mandatory publication requirement was in part for the purpose of facilitating business users in providing their contact details to customers, and in part for the purpose of ensuring that all business profiles displayed comprehensive, reliable, off-Instagram contact details (without exception or the ability to opt-out).

258. Following changes implemented in September 2019, the purpose of this processing was to facilitate the optional display of email and phone information by business account users.

259. With regard to the purpose of including phone and email contact information in the HTML source code, FB-I submits that this served the technical purpose of displaying

²³⁸ It appears that unregistered persons may view a limited amount of content on a public Instagram profile webpage, but will be prompted to log-in or register to have full access to user content.

information in the contact button on the web browser version of Instagram profile pages, as follows²³⁹:

“...in order for a web browser to render the relevant Instagram Web page, the browser must “speak” to an Instagram Web server. This server then sends a set of instructions to the browser for how to display the Instagram Web page, and HTML is the language in which that set of instructions is written. As such, generally speaking, for any information to appear on the Instagram Web page, the Service must write the information in the HTML source code it sends to the web browser.”

260. In connection with FB-I’s decision to make social media posts of child users publicly visible by default, the controller contends that this serves the purpose (as set out in paragraph 250 above) of ensuring a high standard of user experience for new users by allowing connections to be made with other users in the Instagram community. In my view, this default processing arrangement by FB-I also serves the purpose of prompting wider and more extensive sharing of user content, which in turn promotes user engagement with the service, and therefore advances the commercial interests of FB-I in terms of advertising sales.

G.2 Risks of varying likelihood and severity resulting from the processing

261. Articles 24 and 25 GDPR require controllers to take into account the risks (of varying likelihood and severity) for rights and freedoms of natural persons posed by processing of personal data, and to implement measures and safeguards that apply data protection principles and protect the rights of data subjects. Article 35 GDPR requires a Data Protection Impact Assessment in situations where processing is likely to result in a high risk to the rights and freedoms of natural persons. I have therefore considered the risks posed by FB-I’s processing of child user’s personal data, and the measures and safeguards implemented by FB-I in response.

262. 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:

- identity theft or fraud;
- financial loss;
- unauthorised reversal of pseudonymisation;
- significant economic or social disadvantage;
- where personal data of vulnerable natural persons, in particular of children, are processed; and

²³⁹ FB-I’s submission of 18 December 2020, paragraph 54

- where processing involves a large amount of personal data and affects a large number of data subjects.

263. Recital 76 GDPR further outlines how a risk assessment is to be carried out by a controller, as follows:

“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.”

Risks described in FB-I’s Legitimate Interests Assessments

264. On 29 January 2021, and for the purposes of the within Inquiry, FB-I provided the DPC with an updated Legitimate Interests Assessment²⁴⁰ (the “LIA”) regarding its legal basis for provision of services to persons between 13 and 17 years old. While the LIA was completed primarily in the context of FB-I’s obligations under Article 6(1)(f) GDPR, this document also describes the risks associated specifically with the contact information processing and public-by-default processing. The LIA describes, in the following table taken from section 4.2.a of the LIA, the potential “negative impacts” that may result from processing, as follows:

Communication	1	A minor may communicate with (and potentially develop a relationship with) individual(s) who may pose a danger to that minor (e.g. grooming; physical, sexual and emotional abuse; trafficking; etc) and the minor may not be able to identify that danger. This includes risks regarding communication such as inappropriate or unwanted contact, in instances such as those arising from a user choosing to display contact details or the risk that the communication could be taken off platform.
	2	A minor may be bullied online.
	3	A minor may receive inappropriate content.
	4	A minor may be exposed to excessive surveys / product research.
Data retention	5	Messages and content a minor has sent and received from others before their account was deleted may remain visible to those users. This may cause reputational damage or negatively impact the user.
Data access	6	Data about minors collected within the Facebook Products is accessed by an unauthorised person.
Data processing	7	Minors may not understand how their personal data is processed in order to provide them with the Facebook Products.

Figure 8 – Table of “negative affects” taken from section 4.2.a of the LIA of 28 January 2021

²⁴⁰ “Legitimate Interests Assessment (‘LIA’) Processing minors’ data for the provision of the Facebook Products”, 28 January 2021

265. In addition to the above list of seven potential negative effects, the LIA included a corresponding table as part of section 4.2.b, which addressed the “likelihood” and “severity” of each of the seven risks, as follows:

Risk #	Likelihood	Severity
1	We believe the likelihood of this risk is possible . However, Facebook Products allows all users to report bad actors or block people they don’t want to chat with, and we prevent messages from unconnected accounts going directly into users’ inboxes by putting them in the ‘message request’ folder, where they can be easily reviewed and deleted or deleted outright without reading them. The Help Centre provides instructions on how to report and block.	The impact on the minor if contacted by such an individual could result in emotional and/or physical harm and could be severe .
2	We believe the likelihood of this risk is possible . However, we provide self-remediation tools for minors to mitigate these instances, including blocking, reporting and muting functions, which are described in the Youth Portal and in Instagram’s Community Safety Page.	The impact on the minor if subjected to online bullying or inappropriate content could be significant .
3	We believe that this risk is remote . A dedicated support team will respond to flagged content. Further, Instagram has a ‘sensitive content’ measure, whereby photos and videos containing sensitive or graphic content may appear with a warning to let people know about the content before they view it. This warning appears when viewing a post in Feed or on someone’s profile.	If this risk was realised the impact on the minor could be significant, but may not necessarily be severe .
4	We believe the likelihood of this risk is possible given that minors may be given the option to participate in surveys.	Exposure to requests to participate in surveys can impact on a minor’s behavior and they may feel compelled to participate in the survey in order to continue using the Facebook Products. This effect may continue into adulthood. Surveys may also have a subliminal effect on the minor and affect their behavior without them being aware of it. This impact is minimal to significant .
5	We believe the likelihood of this risk is possible . Each of a minor’s contacts could re-share messages and content shared by the minor with others. Facebook has introduced measures to mitigate this risk by educating minor users on the importance of being diligent with what they share online through the Youth Portal. On Instagram, through the new sharing settings launched in January 2021, (as detailed in Section 4.1.c,) relevant minor users on the platform that choose to make their personal account public, are reminded in certain instances of their sharing settings and the ability to change them if needed.	A minor who has left the service may experience embarrassment if messages or content sent when younger remain visible to their contacts. The impact on the former user, depending upon the content of the messages, could be minimal to significant but not severe .

6	We believe the likelihood of this risk is remote . Facebook has appropriate technical security measures in place to prevent unauthorized people from gaining access to data within its systems so the risk of this happening is remote. Controls are in place to protect the data within the Facebook Products.	If this risk occurred the impact could be minimal to significant but not severe .
7	We believe the likelihood of this risk is possible . Data transparency can be difficult to provide to a minor, depending on their age, parental engagement in explaining, and technical literacy. However, Facebook has designed youth-specific transparency content (see screenshots and full text from Youth Portal above at 4.1.c) as well as the range of existing methods for all users to be made aware of their rights around data processing. Further, children are significantly more technically literate than they were a generation ago, with one response to the recent IDPC consultation from children aged 13-14 being: "People underestimate children. We understand the GDPR and our rights. Many people in the class designed apps that run on ad revenue for their business CBA. We researched GDPR and the Cambridge Analytica scandal."	If this risk occurred the impact could be minimal .

Figure 9 – Table taken from section 4.2.b of LIA of 28 January 2021

266. In its submission of 9 August 2021, FB-I submits that the risks identified in the LIA are not "actual" risks for the purpose of the GDPR, but should instead be categorised as "potential" risks, as follows:

"...the Commission overlooks that the risks mentioned in the LIA relate to inherent risks arising from the use of online services by Teens, and the LIA cites them as arising irrespective of an account's audience settings. Secondly, the Commission interprets statements made by Facebook Ireland in relation to identified risks as meaning actual risks rather than merely potential risks (which, as explained in the LIA itself, have been mitigated)."

267. FB-I further submits:

*"The PDD has sought to evaluate these measures and safeguards based on a risk assessment grounded in hypothetical risks and harms. This is evidenced where the PDD states that the Commission is "of the provisional view that these measures are not effective in circumstances where severe **possible** risks are posed by off-Instagram publication of contact information of child users, and **potential** off-Instagram communication which **could** result from publication of contact information" (emphasis added). However, no evidence is put forward to support these conclusions"*

268. A number of issues arise in this regard. First, FB-I is manifestly incorrect in its view that a possible risk is not relevant for the purposes of the GDPR. Articles 24 and 25 GDPR expressly comprehends risk of “*varying likelihood and severity*”. All risks are potential in character, because the term “risk” refers to a situation involving exposure to danger or possible harm; the term risk is not synonymous with “damage” or “harm”. Articles 24, 25 and 35 GDPR do not depend on an assessment of actual material damage caused to data subjects; these provisions are concerned with exposure to danger or possible harm. As such, evidence of risk will not always take the form of examples of actual damage that have resulted from processing (although the NSPCC report referenced below can be considered as evidence of actual damage). An assessment of risk in the context of the GDPR concerns a factual analysis of the exposure to possible harm posed by processing. In this Inquiry, I have considered FB-I’s assessment of risk as set out in the LIA, FB-I’s own submissions, the assessment of risk which emerges from the NSPCC report below, the assessment of risk described in the Berglas Report, and the assessment of risk in Mr Stier’s report to Facebook. All of the above sources refer to factual evidence of risk pertaining to this processing (based on the concrete processing operations conducted by FB-I, and related circumstances) and as such, there is a well-established evidential basis for the below findings.

269. The reason the GDPR provisions focus on “risk” as a trigger for these obligations reflects the legislative intention that controllers should take prior steps to identify and mitigate risk, before damage occurs, in conformity with the principle of accountability. Even where a controller may have mitigated a risk to some extent, it remains a relevant risk for the purposes of the GDPR, to the extent that the controller was and is obliged to implement corresponding measures and safeguards, and to be accountable for its compliance with the GDPR regarding such measures. A controller cannot side-step its obligations under Articles 24, 25 and 35 GDPR by denying the existence of risk on the basis of mitigating actions taken; the process of identifying and mitigating these risks takes place within the ambit of the GDPR. A controller must be able to demonstrate the measures and safeguards implemented with regard to processing. FB-I’s submission regarding “*merely potential risks*” is therefore based on an incorrect construction of the GDPR, because a possible risk is an actual risk; the use of the term *possible* in this context goes to the likelihood of the risk resulting in damage. The term *possible risk* as used in this Decision does not mean that there is a only a possible chance that the risk itself exists; it means that the likelihood of the risk leading to actual damage is not remote or impossible (and nor such damage inevitable). What is more, it is clear that FB-I’s own LIA uses the term *possible risk* in this sense (if nothing else, this is clear from the other assessments of risk in section 4.2.b of the LIA, which refers to the possibility of certain risks as being *remote* – i.e. less likely than *possible*).

270. I am therefore satisfied that FB-I's submission of 9 August 2021 is incorrect to the extent that it asserts that possible risks set out in the LIA should be disregarded for the purpose of Articles 24, 25 and 35 GDPR.

271. FB-I also submits above that the risks identified in the LIA are inherent to the operation of online services by child users, whether or not an account is public or private. FB-I is of the view that these risks are essential base-level online risks, which are not caused by or unique to Instagram. However, this statement amounts to a tacit acknowledgement by FB-I that the risks specified in the LIA are inherent to the provision of the Instagram service to child users. If this is the case, then such risks should be accounted for as appropriate under Articles 24, 25 and 35 GDPR – nothing in the GDPR suggests that a controller need not address pervasive societal risks (which exist in the context of processing).

272. FB-I also contends that the LIA risks are “*merely potential*”. This statement is directly contradicted by the actual wording of both LIAs provided by FB-I, which contain (in sections 4.2.a) explicit lists of “*possible negative impact(s) of the processing on individuals*” (i.e. actual, not hypothetical, possibility of harm to individuals – a concept which is synonymous with risk for the purpose of the GDPR). Both LIAs proceed to set out (in section 4.2.b) statements of the “*the likelihood and severity of any potential impact(s)*”. With regard to the first risk listed in section 4.2.a of the LIA (concerning contact between dangerous individuals and child users), the LIA assesses this risk as being “possible” (as compared to “remote” – a conclusion on likelihood found elsewhere in the LIA for other risks). It is obvious that sections 4.2.a and b are drafted in order to identify actual risks, and to assess the “likelihood and severity” those risks for the purpose of the GDPR. It is therefore entirely contradictory for FB-I to now assert that a possible risk, which is associated with severe consequences (according to the express conclusions of two previous risk assessments by FB-I), is in fact not an actual risk, but is merely a species of hypothetical risk which can be discarded for the purpose of GDPR compliance. I can see no reasonable basis for FB-I's suggested interpretation of its own LIA; a plain reading of the conclusions of the LIA supports the view that FB-I itself identified possible risks with severe consequences in the context of providing its service to child users. To be clear, FB-I has not sought to withdraw or correct any content of the LIA; to the contrary, FB-I now seeks to rely²⁴¹ on the risk assessment carried out in this context as the basis for its compliance with Article 35 GDPR (notwithstanding FB-I's view that the LIA does not identify “*actual risks*”). Accordingly, I do not accept FB-I's view that the clear risks identified in the LIA are to be disregarded for the purposes of assessing its obligations under Articles 24, 25 and 35 GDPR.

273. The risks identified in section 4.2.a of the LIA also include the risk that “*Data about minors collected within the Facebook Products is accessed by an unauthorised person*”. FB-I

²⁴¹ FB-I's submission of 9 August 2021, paragraphs 80 to 82

concludes in the LIA that the possibility of such a risk is remote, on the basis that FB-I has “appropriate technical security measures in place to prevent unauthorized people from gaining access to data within its systems”²⁴². However, this does not account for the possible risk of unauthorised web scraping of contact information of child users, which would not have been prevented by Instagram’s security measures, because information was intentionally published in the HTML for profile pages of business accounts, and also visible as plain text on Instagram profile pages. I am satisfied that such processing resulted in a significant and possible risk to the rights and freedoms of child users, as a result of the possible use of phone and email information for the purposes of fraud and impersonation. This risk is greater with regard to child users, who may have inadvertently published their personal contact information on a business account profile webpage, without fully appreciating the risk of unauthorised collection of this information by third-parties.

NSPCC Reports concerning Instagram

274. Further to the risks identified by FB-I in its LIA, it is a matter of public record that online sexual offences occur in the context of the Instagram service in the European Union. For example, in 2017 the United Kingdom introduced the criminal offence²⁴³ of sexual communication with a child. FB-I was the data controller for the Instagram service in the UK at this time. A UK-based charity, the National Society for the Prevention of Cruelty to Children (NSPCC) subsequently obtained statistics from police forces in England and Wales regarding “police-recorded offences involving adults accused of having sexual communication with a child”. In a subsequent report, the NSPCC described the extent of this type of criminal offence in the UK, as follows:

“Technology-facilitated grooming has become a major challenge. In the first 18 months since it became an offence to send sexual communication to a child, there were over 5,000 offences recorded by the police in England and Wales. In 70 per cent of instances where the data were recorded, grooming took place on Facebook, Snapchat or Instagram. This is despite such sites, as the largest social networks, having considerable resources to tackle abuse occurring on their platforms...As part of the NSPCC’s FOI request, police forces in England and Wales were asked what means of communication were used to commit offences of sexual communication with a child. One offence could involve multiple instances of communicating with a child, and multiple means of communication. Police were not always able to provide information on the means of communication used. However, for the 3,418 instances where the information was provided:

- *27 per cent of instances involved Facebook or Facebook messenger;*

²⁴² Section 4.2.b of the LIA

²⁴³ UK Sexual Offences Act 2003, section 15A

- *25 per cent involved Instagram;*
- *18 per cent involved Snapchat;*
- *7 per cent involved text messages; and*
- *4 per cent involved WhatsApp.*

These five means of communication together accounted for 81 per cent of all instances. In total 80 different means of communication were named.” (emphasis added)

275. In its submission of 9 August 2021, FB-I attempted to downplay the risks identified by the NSPCC report. In particular, FB-I submitted that the report was not specific to Instagram, and was geographically limited to the United Kingdom. However, this report was specific with regard to the number of offences which were associated with Instagram, and in particular, this report found that for the 3,418 offences where the means of communication was recorded, 25% of these cases involved communications on Instagram. In my view, this information is specific with regard to Instagram, and discloses a significant number of serious incidents (i.e. criminal offences of sexual communication with a child, where Instagram was used as the means of communication), which constitutes clear evidence of risk for the purpose of Articles 24, 25 and 35 GDPR.

276. FB-I also contends²⁴⁴ that the offences described in the NSPCC report may not be relevant in this context, because the report:

“...does not indicate, for example, whether these offences involved an individual known to the user as compared to instances arising from contact from a stranger via the social media platform -- or from interactions which may have originated off-platform. Simply put, the report fails to demonstrate any causal link between the Account Audience Setting at issue in this Inquiry and the harms alleged.”

277. In this regard, FB-I does not appreciate the relevance of the NSPCC report in the context of this Inquiry; the NSPCC report is clear evidence of risk which exists in the context of the Instagram platform (irrespective of whether the contact is made by a stranger, or by a person otherwise known to a child user). The NSPCC report itself further notes²⁴⁵ that these statistics are likely to be an incomplete picture of actual harms, given that they relate only to criminal offences that have been detected by UK police. FB-I’s contention that the statistics on offences committed using Instagram as a means of communication are insufficiently precise with respect to the public-by-default processing and the contact information processing is beside the point; the severe risk to child users which is disclosed by the NSPCC report constitutes a pervasive risk insofar as the Instagram

²⁴⁴ FB-I’s submission of 9 August 2021, Annex A

²⁴⁵ “How safe are our children? 2019” NSPCC, page 8

service is provided to child users, and as such, it is a risk to be taken into account for the purpose of Articles 24, 25 and 35 of the GDPR with regard to the processing at issue.

278. Notwithstanding the well-documented risks set out in the LIA prepared by FB-I, and the numerous recorded criminal offences which have been associated with the Instagram platform in the UK, FB-I contends that the actual level of risk associated with this processing was “*not high*”.

279. In its submission of 9 August 2021 FB-I also contends²⁴⁶ in relation to the public-by-default processing that “*more often, online bullying/harm occurs as a result of harmful communications from people the user knows from an offline setting*”. The academic sources cited by FB-I in this regard support the view that online harm is more likely to be caused by persons known to the victim. At the same time, the same articles cited by FB-I state²⁴⁷ that “*...these results do not imply that strangers never engage in cruel online actions toward adolescents. Indeed, such cases do occur and sometimes with tragic consequences*”. I do not dispute the potential for harmful interactions between Instagram users and their approved followers (and indeed, the inadvertent publication of email or phone contact details of a child user may pose an additional risk of bullying by persons known to them, insofar that it would allow someone to send anonymous messages to a person, off-Instagram). There is evidence to suggest²⁴⁸ that as many as one third of child users communicate with people online that they have not previously met face-to-face, and one in five child users between the ages of 12 to 14 report that they have met someone in person that they first met online (in some cases resulting in unpleasant experiences for these children). Given the serious potential consequences for the child users who may be contacted by dangerous individuals (and allowing for the fact that such users may constitute a minority of the overall population of child users on Instagram) I am satisfied that this is a material risk to be taken into account for the purposes of Articles 24, 25 and 35 GDPR.

The Berglas Report

280. On 16 August 2021, FB-I furnished the DPC with an additional report, prepared by Mr Austin Berglas of BlueVoyant LLC (the “**Berglas Report**”) in response to certain issues raised in the PDD. This report was prepared by Mr Berglas, having been engaged as a consulting expert by Mason Hayes & Curran Solicitors on behalf of FB-I. Mr Berglas’ report was produced on the sole initiative of FB-I, and was not requested by the DPC. Mr Berglas states that he was asked to provide his opinion on “*any risk of user harm resulting from the contact details (i.e. email or phone number) of business account users being*

²⁴⁶ FB-I’s submission of 9 August 2021, Annex A and footnotes 151

²⁴⁷ Felmlee and Faris, *Toxic Ties: Networks of Friendship, Dating, and Cyber Victimization*, Social Psychology Quarterly (2016), page 257

²⁴⁸ Online experiences of children in Bulgaria: risks and safety (authors: Marko Hajdinjak, Petar Kanchev, Emanuil Georgiev and Georgi Apostolov, Bulgarian Safer Internet Centre; 2017), page 12

publicly available on IG, such as through the contact information button on the profile of IG users who chose to switch to a business account or as a result of the default settings of such a business account making those contact detail public by default and, specifically, to analyze any risk of harm to Teen Users who may have converted their profile to a business account". Mr Berglas states that he is Global Head of Professional Services at BlueVoyant, LLC, a cybersecurity consulting company based in New York. Mr Berglas describes his professional experience as follows:

"Before coming to BlueVoyant, I served as the Assistant Special Agent in Charge of the Cyber Branch of the Federal Bureau of Investigation's ("FBI") New York Field Office. In that position I oversaw all cyber criminal and national security investigations in the largest cyber branch of the FBI. I also established the Financial Cyber Crimes Task Force, the FBI's first joint effort with the New York City Police Department and the Metropolitan Transportation Authority to combat threats and other forms of financial cybercrime affecting New York City and the United States."

281. Mr Berglas states that he has no conflicting interests with regard to the subject of this Inquiry, and further states that he is subject to a *"duty as an independent expert...to assist as to matters within my field of expertise in the course of the Inquiry in an independent manner"* and submits that he has *"not, without forming an independent view, included or excluded anything in my report which has been suggested to me by others"*. The Berglas report has a strong emphasis on conditions that pertain to the United States of America, with little content that refers specifically to the European Union, or other jurisdictions where FB-I acts as controller.

282. Mr Berglas' first contention relates to the contact information processing. Mr Berglas submits that making phone numbers and email addresses publicly available does not increase an individual's risk of identity theft, for the reason that criminals need other information points, such as national ID numbers, to perpetrate identity theft. Mr Berglas states that accurate contact information is not typically used in the context of identity theft, because criminals will more often use fake contact information with other more sensitive data when committing fraud.

283. In this context, Mr Berglas invites the DPC to consider the examples of categories of sensitive personal data as specified by the U.S. Federal Trade Commission in relation to identity theft. Mr Berglas states that the materials provided by the U.S. Federal Trade Commission contain *"no mention of any basic contact information as a criterion for identity theft. None of the requisite information for committing identity theft was made available here"*.

284. In this regard, the Berglas Report states that a social security number would be considered sensitive personal data from the perspective of fraud, whereas a phone number would *"not meet the requisite information needed to commit identity theft"*.

However, apart from the direct use of phone/email contact information for the purpose of making fraudulent financial applications, contact information may also pose risks when combined with other information. These types of persistent identifiers are frequently used for registration purposes across numerous online services. For example, in a 2016 media article titled “A 10-Digit Key Code to Your Private Life: Your Cellphone Number” published in the New York Times²⁴⁹, Mr Edward M. Stroz, a former Agent with the United States Federal Bureau of Investigation, is quoted as saying that a phone number has become “*kind of a key into the room of your life and information about you*,”. This article also appears to include a quote from Mr Berglas himself, as follows:

*“...investigators find that **a cellphone number is often even more useful than a Social Security number because it is tied to so many databases and is connected to a device you almost always have with you**, said Austin Berglas, a former F.B.I. agent who is senior managing director of K2 Intelligence, a private investigator.*

“The point is the cellphone number can be a gateway to all sorts of other information,” said Robert Schoshinski, the assistant director for privacy and identity protection at the Federal Trade Commission. “People should think about it.””
(emphasis added)

285. While Mr Berglas was referring in the above article to the use of phone numbers by private investigators, and not criminals, the point made is also valid in the context of fraud and impersonation; a person’s phone number is a strong identifier in the context of many other online services and databases, and allows for direct access to a person, giving rise to risk of social engineering fraud.

286. Mr Berglas may be correct in his assessment that accurate phone and email contact information is not typically used in certain types of identity fraud, however, contact information is relevant to other types of fraud and impersonation, including phishing, sim-swapping, and social-engineering based fraud. Criminals may use accurate personal phone and email information in combination with separately obtained information (for example, passwords which have been the subject of a security breach), for the purpose of carrying out fraud.

287. I note in this regard a study conducted by the European Commission in 2020, which found that 56% of Europeans had experienced some form of fraud or scam over the last two years.²⁵⁰ Respondents noted that by far the most common channel through which they experienced fraud was “via an email” (43%), followed by “via a phone call on your

²⁴⁹ “ A 10-Digit Key Code to Your Private Life: Your Cellphone Number” Steve Lohr, New York Times, 12 November 2016

²⁵⁰ https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf
p9

mobile” (15%); “via a phone call on your landline phone” (14%) and “via text message” (5%)²⁵¹. The report also found that “those who experienced identity theft relatively often experienced this scam or fraud by phone (39% did so)”²⁵² Finally, the Commission noted that:

*“It is [...] crucial to take into account that in general consumer scams and fraud are considered to be largely under-reported and online scams and fraud even more so. Some people might not know to whom to report scams and fraud, might not feel it is worth the effort to report, or might not even be aware that they are victim of a crime.”*²⁵³

288. The findings of the European Commission regarding public perceptions of the pervasiveness of fraud correspond with several recent surveys by Ipsos, which show that respondents around the world view threats to their privacy arising from fraud²⁵⁴ and cybercrime²⁵⁵ as significant and growing risks. It is evident that fraud and criminality are widely regarded as significant and under-reported risks in the digital environment both in Europe and internationally.

289. Turning to the incidence of fraud specifically on the Instagram platform, I note a recent article entitled “*Instagram favourite site for scammers*” published in the British newspaper The Times²⁵⁶ which reports that, according to figures from TSB Bank plc, Instagram has become “by far” the most popular platform for investment-related fraud. Specifically, the article noted that:

*“Of all investment fraud reports to TSB this year, **Instagram-based scams made up 62 per cent**, Snapchat 11 per cent, Google 10 per cent and Facebook 8 per cent. However, no customers had reported falling victim to fraud through Google since August 30, whereas **last month the proportion of reports relating to Instagram rose to 68 per cent.**”*²⁵⁷ (emphasis added)

²⁵¹ Ibid, p31

²⁵² https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

²⁵³ Ibid, page 7

²⁵⁴ For example, a 2019 survey by Ipsos found that 75% of respondents across 28 countries consider “being hacked for fraudulent/espionage purposes” to be a “real” threat, the highest aggregate figure for any recorded threat in the survey: <https://www.ipsos.com/sites/default/files/ct/news/documents/2019-11/a-more-dangerous-world-fear-2019.pdf>

²⁵⁵ A 2019 survey by the Centre for International Governance Innovation/ Ipsos across 25 countries found that 53% of respondents are more concerned about their online privacy than last year; of these, 81% reported that “cyber criminals” have contributed to their increased levels of concern: <https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf>

²⁵⁶ “Instagram favourite site for scammers” David Byers, The Times, 26 November 2021

²⁵⁷ Ibid

290. The direct and specific utility of phone and email contact information for the purposes of fraud was emphasised by Instagram itself in the context of a 2017 leak of phone and email contact details, caused by an Application Programming Interface bug. A subsequent message published²⁵⁸ by Mr Mike Krieger (Co-Founder and then CTO of Instagram) on 1 September 2017, stated:

*“...we want to let you know that we recently discovered a bug on Instagram that could be used to access some **people’s email address and phone number** even if they were not public. No passwords or other Instagram activity was revealed.*

We quickly fixed the bug, and have been working with law enforcement on the matter. Although we cannot determine which specific accounts may have been impacted, we believe it was a low percentage of Instagram accounts.

*Out of an abundance of caution, we encourage you to be vigilant about the security of your account, **and exercise caution if you observe any suspicious activity such as unrecognized incoming calls, texts, or emails.**” (emphasis added)*

291. Although the 2017 incident is not relevant to the scope of this Inquiry, Mr Krieger’s statement demonstrates the fact that phone and email contact information can be used directly in the context of phishing and social engineering fraud. Subsequent to this leak, phone and email information leaked as a result of this Instagram bug was reportedly²⁵⁹ provided for sale by criminals as part of a publicly accessible database.

292. The Berglas report also addresses the risk of so-called “port out” or “sim-swapping” fraud, whereby criminals can redirect a person’s phone number to a different device, in order to intercept two-factor authentication messages and gain access to the user’s accounts for fraudulent purposes. Mr Berglas contends that the risk of sim-swapping is low in this case, as follows:

“account takeover and SIM-swapping (hijacking an individual’s phone number) require compromised passwords and/or a substantial criminal effort. It is highly unreasonable to conclude that exposed contact information would feasibly lead to impersonation efforts.”

293. I note that when writing in another context²⁶⁰, Mr Berglas has stated:

²⁵⁸ Published online at <http://blog.instagram.com/post/164871973302/170901-news>

²⁵⁹ <https://www.thedailybeast.com/hackers-make-searchable-database-to-dox-instagram-celebs>

²⁶⁰ “A Concerning Proliferation of SIM-Swapping Fraud in Europe” Austin Berglas, Infosecurity Magazine, 7 July 2020, available online at <https://www.infosecurity-magazine.com/opinions/proliferation-sim-swapping-fraud/>

*“As SIM swapping requires substantial effort and costs from attackers, we are seeing high net worth individuals and people in positions of corporate, government, or **social influence** increasingly being targeted”* (emphasis added)

294. I note that some child users of Instagram may have operated prominent social media profiles, as described by FB-I in its submissions²⁶¹. It also appears²⁶² that sim-swapping has been used in recent years to steal “valuable” Instagram accounts (e.g. eye-catching user names claimed by early adopters of Instagram, which can be resold for profit).

295. Current advice²⁶³ on prevention of sim-swapping fraud, as issued by the U.S. Federal Communications Commission, also emphasises the need to keep personal phone numbers private, as follows:

*“Don’t overshare: Guard personal details that can be used to verify your identity – such as the last four digits of your Social Security number, **your phone number**, your date of birth, the make and model of your car, your pet’s name, or your mother’s maiden name. **And keep that information off social media.**”* (Emphasis added)

296. Europol has similarly issued advice²⁶⁴ warning that people should “*Limit the amount of personal data you share online*” as a precaution against sim-swapping fraud. While I accept that sim-swapping is a less common form of fraud, it is not unreasonable to conclude that certain high-profile child users of Instagram could have been exposed to this risk by the publication of their phone or email information.

297. In conclusion, I am not convinced by Mr Berglas’ first submission, that publication of personal phone and email contact information would not lead to increased risk of identity theft. Mr Berglas may be correct in his view that phone/email contact information would not typically be used when making a fraudulent financial application, however, the Berglas Report fails to account for obvious wider risks which result from the publication of email and phone information, and in particular, risks relating to the widespread use of these identifiers for other online services, and the risk that a child user could be contacted directly in the context of phishing or other forms of social engineering fraud.

298. The second submission in the Berglas report concerns the risk of online grooming of children (i.e. a process in which a predator communicates with a child over time to gain their trust, in the context of child abuse or exploitation). Mr Berglas submits, based on

²⁶¹ FB-I’s submission of 18 December 2020, paragraphs 37 and 38

²⁶² “Instagram Bans Hundreds of Accounts With Stolen User Names” Taylor Lorenz, New York Times, 4 February 2021

²⁶³ “Port-Out Fraud Targets Your Private Accounts”, U.S. Federal Communications Commission, available online at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>, last accessed 12 October 2021

²⁶⁴ <https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers>

his experience as a Special Agent with the U.S. Federal Bureau of Investigation, that online grooming is less common than offline grooming. He states that this process typically takes place over 1-2 months, and will not initially involve requests for personal contact information. In particular, Mr Berglas states:

*“...Safekids, an online Internet safety site, states this fact explicitly: **“asking for personal info of any kind – usually happens at a later [grooming] stage, after the target’s feeling comfortable with the groomer.”** This means groomers are utilizing other forms of communication before requesting things like email or phone number from a child.”*

299. The above statement in the Berglas Report is regrettably taken out of context, and selectively quotes the organisation in question. The complete quote²⁶⁵ by the Safekids organisation is taken from a website which gives examples of specific types of grooming, as follows:

*“**“What’s your phone number?”** (asking for personal info of any kind – usually happens at a later stage, after the target’s feeling comfortable with the groomer – but all online kids know not to give out personal info online, right?!)”* (emphasis added)

300. Safekids further warns that predators may attempt to communicate using other modes, including phone, as follows:

*“**“Let’s go private.”** (leave the public chatroom and create a private chat or **move to instant-messaging or phone texting**)”* (emphasis added)

301. It is therefore obvious that contrary to Mr Berglas’ selective quotation of this organisation, Safekids actually advises that phone contact information can be sought and used by predators in the context of grooming. The Berglas Report does not account for this specific risk, and therefore fails to acknowledge that contact information may be used in the wider context of grooming (apart from “cold contact” situations) because predators may simply use this information at a later stage of the grooming process.

302. I also note in this context that phone numbers act as strong personal identifiers in the online context, as used by “over-the-top” communication services. Instant messaging applications, and other modes of online communication, will often use phone numbers or email addresses held by one user as a mean to identify other “connected” users, who may be known to each other. In this way, public phone or email contact information could be used to identify a child user on another online platform, facilitating off-Instagram communication. For example the “WhatsApp” messaging application (also

²⁶⁵ <http://www.safekids.com/how-to-recognize-grooming-2/>

owned by Meta Platforms, Inc.) uses a person's phone number as the basis for an in-app identifier which in turn is used to link WhatsApp users as contacts.

303. Moreover, the narrow framing of the issue by the Berglas report fails to satisfactorily consider the high level of general risk children face in the digital environment: A recent survey by the WeProtect Global Alliance of 5,000 young adults on their past online experiences as children revealed that 54% of respondents reported experiencing at least one form of "online sexual harm"²⁶⁶ before they turned 18. Specifically, 34% were asked to do something sexually explicit online; 29% received explicit content from a stranger, and; 25% had an explicit online interaction with a stranger who asked them to keep it secret.²⁶⁷ The same report also contained an analysis of conversations by online predators on "technology topics" in several chat forums hosted on the dark web. These conversations, which took place in February 2021, focussed on tools and strategies for facilitating the exploitation of children online. Of the conversations analysed as part of the study, a plurality (32.8%) concerned "social media platforms".²⁶⁸

304. The findings of the WeProtect report illustrate first that children are more likely than not to experience at least one form of online sexual harm over the course of their childhood, and, as a result, clearly face a high level of general risk of online sexual harm in the digital environment. Second, the report also shows that online predators regard social media as an effective means for meeting and grooming children online. Third, the technical subject matter of many of these conversations (e.g. "secure tooling", "content storage & exchange", "cloud file share", "capping techniques & tools" etc.) which took place on websites on the dark web that are not accessible via conventional web browsers implies an above-average level of technical literacy, contrary to Mr Berglas' suggestion that online predators "*cannot be realistically characterized*" as such.²⁶⁹

305. In its submission of 9 August 2021, FB-I states²⁷⁰ that it "*partners closely with the National Center for Missing and Exploited Children (NCMEC) in reporting instances of child exploitation from around the world*". In 2017, the NCMEC conducted an analysis²⁷¹ of 5,863 "cyber-tipline reports" (i.e. suspected instances of child sexual exploitation) received in 2015. This study found that:

- 98% of reported offenders were seemingly unknown to the children in real life;

²⁶⁶ The online harms in the survey were: being sent sexually-explicit content from an adult; being asked to keep a sexually explicit online relationship with an adult/stranger a secret; having a sexually explicit image shared without their consent; being asked to do something sexually-explicit online they were uncomfortable with

²⁶⁷ <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf> p15-16

²⁶⁸ <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf> p28

²⁶⁹ The Berglas Letter, Page 2

²⁷⁰ FB-I's submission of 9 August 2021, paragraph 98

²⁷¹ <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel.pdf>

- 90% of the reports concerned offenders' direct communication with children (or an attempt to do so).
- 71% of these incidents were reported by internet companies.
- 24% of the reports indicated that images of the child victim were shared with the offender, either by the child or another offender;
- 12% of the reports mentioned plans or suggestions to meet up;
In 2% of cases, the child experienced negative effects as a result of the online enticement such as anxiety, depression or self-harm. In a handful of cases, either the child or the offender threatened some form of violence at the prospect of the termination of the relationship (e.g. upon discovery by parents).

306. It is evident from these figures that, even if it is true as Mr Berglas contends, that online grooming is less common than offline grooming, this does not negate the clear and foreseeable risk of online grooming of children by predators in the digital environment. In its submission on the PDD, FB-I has pointed to its engagement with the WeProtect Global Alliance and the NCMEC as examples of its measures to address child safety and exploitation risks. Given its engagement with these organisations over many years, I find it unlikely that FB-I was simultaneously unaware of their research demonstrating the severe risks of grooming that children face online as outlined above.

307. In conclusion, the Berglas report has a singular emphasis on the risk of "cold contact" by predators. However, the more likely risk is that phone and email contact information could be misused as part of a longer-term grooming process, as an alternative mode of communication with a child (a risk acknowledged by the Safekids organisation cited by Mr Berglas). I am therefore not convinced by Mr Berglas' submission that disclosure of phone and/or email contact information would not prove a risk to child users in the context of online grooming.

308. Mr Berglas states that children are "digital natives" who would be vigilant against unsolicited communications in the form of "cold contact" by predators. In particular, Mr Berglas submits:

"Cold contacting is the act of making an unsolicited call, text, or email in an attempt to sell a good or service. Robocallers, spam farms, and sales teams launch emails, phone calls, and text messages in vast numbers. We have all learned to ignore, block, and report these nuisances. Children are no different. Digital natives, in fact, are typically savvier than adults in recognizing and ignoring unsolicited contact on social media, email, and mobile platforms. Our electronic devices often flag these messages as spam, and many have built-in features to report them as such. We are all, by now, well-accustomed to the cold calls that falsely solicit our need to renew an auto insurance plan."

309. The assertion that child users are more sophisticated and risk averse is not always borne out in practice, and this assumption runs contrary to the precautionary objectives described in Recital 38 GDPR. It appears from FB-I's submissions and the Berglas report that the controller assumes child users to have a high standard of digital literacy. I note that academic commentary does not always support this view; for example, Eynon²⁷² states:

"The digital native discourse effectively celebrates all young people's uses of technology in an uncritical fashion, and does this alongside an uncritical and deterministic model of technology, where all technology is exciting and positioned as the factor that will drive our future society. This leads to an overriding acceptance of the status quo and a deterministic view of technology that does not help young people or those trying to support them."

310. In practice, child users of social media services have varying levels of digital literacy. For example, a national representative survey conducted in 2016²⁷³ in Bulgaria (a state where FB-I has acted as controller for the Instagram service) identified five key competency gaps in digital and media literacy of children, including *"(u)nderdeveloped digital safety skills of older children"*. The authors of this survey concluded:

"The older children become, the more likely it is for their devices to be infected by a virus (16% of 9-11 year olds; 30% for 12-14 year olds; 35% of 15-17 year-olds). In addition, even though, relative to 2010, an increased percentage of Bulgarian children reported the ability to change their social network's profile settings (64% in 2010 vs. 73% in 2016), the percentage of public profiles among them hasn't changed (31.7% in 2010 vs. 31.5% in 2016). The percentage of public profiles for 12-14 year olds was the highest (40%) of all age groups. This increase of online risks for older children correlates with more internet usage, but it also correlates with decreased parental mediation and insufficient internet safety education in schools."

It is therefore not the case that all children can be assumed to have high levels of digital literacy; digital literacy is learned and not inherent to child users.

311. Mr Berglas further submits that mobile phones are not typically used by predators, because predators are aware that SMS messages and other phone records can be traced by law enforcement agencies. In this regard, it is important to note that online predators would not be provided with phone and email contact information in isolation; this information would be associated with a public Instagram account, which would allow for direct online communication with the child user in conjunction with the additional modes

²⁷² OECD/Rebecca Eynon (2020), "The myth of the digital native: Why it persists and the harm it inflicts", in Burns, T. and F. Gottschalk (eds.), *Education in the Digital Age: Healthy and Happy Children*

²⁷³ Are Digital Natives Digitally Literate? Insights from a national representative survey (authors: Petar Kanchev, Marko Hajdinjak, Emanuil Georgiev and Georgi Apostolov, Bulgarian Safer Internet Centre; 2017)

of communication made possible by phone and email contact information. Predators would not need to use traditional phone or SMS modes of communication to contact a child: a phone number or email address could also be used to identify and communicate with a child user on other social media or messaging apps, because many applications offer a function to “connect with your contacts” using phone or email information you hold.

312. Mr Berglas also submits that online predators will typically use Virtual Private Networks to hide their online identity. Mr Berglas submits that *“A child predator places themselves at much greater risk of being caught by engaging a child through SMS than they do via social media or other online platforms – especially before having earned the minor’s trust”*. While this statement may be accurate with regard to conventional SMS messages, it fails to account for fact that VPNs could also be used to hide a predator’s location when sending emails, or when using other modes of online communication which rely on phone and email contact information as identifiers for users.

313. With regard to the disclosure of contact information in the HTML source code of profile pages, Mr Berglas submits that this would not normally be a *“a realistic source of information by which potential child predators would select their targets”*, because this form of access to information would require above-average technical skill, and because in most cases predators are known to children. Mr Berglas therefore submits that obtaining information from HTML for the purpose of “cold-calling” a child would not be a likely series of events.

314. With regard to the other risks associated with HTML publication of contact information, Mr Berglas states:

“I have been asked to opine on the risk of impersonation with respect to the inclusion of contact information in the Instagram business accounts HTML code. In brief, I do not see any plausible threat of impersonation. If a malicious actor has knowledge of an individuals’ contact information, that does not grant them the ability to access an email account inbox or hijack an individual’s cell phone capabilities. To the contrary, account takeover and SIM-swapping (hijacking an individual’s phone number) require compromised passwords and/or a substantial criminal effort. It is highly unreasonable to conclude that exposed contact information would feasibly lead to impersonation efforts.”

315. The inclusion of contact information in the HTML source code for profile pages was first raised as an issue by Mr Stier, in his security report to Facebook. In particular, Mr Stier stated that he had reviewed more than 18000 profile pages of Instagram users in the EU by accessing data in the source code of webpage profiles. Of these 18000 users, Mr Stier found that over 1000 users had phone contact information in the HTML source code, and more than 4000 profiles had email addresses in the source code. Mr Stier subsequently

advised Facebook that this information could easily be accessed, and posed a risk in terms of scraping of personal contact information by third parties. While I accept that FB-I has implemented certain measures to prevent scraping of account data (discussed further below), it nevertheless appears that there was no technical impediment to Mr Stier's collection of contact information for thousands of EU-based Instagram users. As such, I am of the view that undetected scraping of contact details was a possible risk resulting from the inclusion of contact information as plain text in the HTML source code of web-based Instagram profiles. I am further of the view that this potential scraping would have involved a relatively low level of effort on the part of a third party, as evidenced by Mr Stier's security report to Facebook.

316. While I accept Mr Berglas' submission that the inclusion of contact information in the HTML source code of web-based Instagram profiles may not have increased the specific risk of grooming, I am not convinced by his submission regarding other forms of fraud. More common types of fraud, including phishing and social engineering, could plausibly exploit user's contact information obtained in this manner; while contact information may not be sufficient alone for the purposes of fraud, phone and/or email contact information could be targeted for phishing and other forms of social engineering fraud.

317. In conclusion, having considered the Berglas Report in full, I am not satisfied that the report is a comprehensive treatment of risk arising from the contact information processing or the public-by-default processing. Accordingly, I do not accept Mr Berglas' submissions regarding the purported low level of risk associated with the processing at issue.

Conclusion

318. Having had regard to the nature, scope, context and purposes of processing (as set out in part G.1 above), as well as FB-I's own risk assessment set out in the LIA, the Berglas Report, and public sources of information on criminal offences which have been recorded in the context of the Instagram service, I am satisfied that both types of processing which are the subject of this Inquiry pose high risks to the rights and freedoms of child users, for the purposes of Articles 24, 25 and 35 GDPR.

G.3 Technical and organisational measures, and safeguards implemented by FB-I with regard to processing

319. Articles 24 and 25 GDPR require the implementation of **technical and organisational measures** in order to comply with the accountability principle under the GDPR, and to ensure data protection by design and by default. Controllers are also required to implement **safeguards** to protect the rights of data subjects pursuant to Article 25(1) GDPR, to ensure data protection by design.

320. It is not within the remit of the DPC, or the scope of the GDPR, to make binding legal determinations on whether a controller has created a safe online platform for child users. Nevertheless, consideration of the **measures and safeguards** adopted by FB-I in connection with Articles 24 and 25 are relevant issues for determination, which are addressed in Part G.3 of this Decision.

321. On 21 March 2021, FB-I announced²⁷⁴ a suite of new protections for child users of Instagram. In particular, FB-I announced:

- a new feature that prevents adults from sending messages to people under 18 who don't follow them;
- prompts, in the form of safety notices, to warn child users when an adult who has been exhibiting potentially suspicious behaviour is interacting with them in direct messages on Instagram; and
- a new step when someone between the ages of 13 and 18 signs up for an Instagram account that gives them the option to choose between a public or private account.

322. In response to the PDD, FB-I further notified the DPC in its submission of 9 August 2021 of additional service modifications, set out below at paragraphs 328 to 336. For the purposes of this Inquiry, I note FB-I's contention²⁷⁵ that its processing was already "*fully in line with its obligations under the GDPR*", prior to the March 2021 changes. The March 2021 changes to the Instagram service (and changes made subsequent to the PDD) do not fall within the scope of this Inquiry, and I assume that these changes are without prejudice to FB-I'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.

FB-I's measures and safeguards regarding the processing at issue

323. In its submissions to the DPC, FB-I maintains that it designed and implemented a safe platform, where child users and older users can interact. In particular, FB-I seeks to rely on the following measures:

"Facebook Ireland's emphasis on creating a safe environment for all Instagram users – including Teens – begins with Instagram's terms and policies, which generally set the minimum age to have an Instagram account at 13. Facebook Ireland promptly deletes an account where it is able to reasonably ascertain that a user's age is below 13. Facebook Ireland also prohibits anyone from impersonating others, providing

²⁷⁴ <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community>

²⁷⁵ FB-I's submission of 18 December 2020, paragraph 32

inaccurate information, and doing anything unlawful, misleading, or fraudulent or for an illegal or unauthorized purpose. Instagram's Community Guidelines, a set of safety-centric rules that outline what is and is not allowed on Instagram, prohibit harmful content, interactions, and behaviour on Instagram, and are intended to keep the platform safe for all users, regardless of age.

324. FB-I contends²⁷⁶ that it also provides a suite of in-app safety tools and privacy and security features aimed at ensuring platform safety, including the following:

- Safety tools to block, mute, or restrict unwanted interactions with other Instagram users;
- Comment controls that allow users to control the comments they see on Instagram;
- Privacy features to control their visibility on Instagram (e.g. private accounts and audience controls);
- Controls regarding direct messages, including restricting who can send messages;
- Tools to view and manage personal data;
- “Time Spent” tools to monitor app usage time;
- In-app reporting tools for users to report posts, accounts, comments, and direct messages that they feel are inappropriate, or go against the Instagram Community Guidelines; and
- Automated systems and technologies to prevent abuse.
- Education resources for child users and parents about Instagram's in-app safety tools and privacy and security features.

325. Together with its submission of 27 October 2020, FB-I provided the DPC with copies of the educational and information resources provided to child users and parents, including the following:

- The Instagram Community Guidelines;
- Webpages from the Help Centre concerning private account settings, hiding activity status, and editing contact information of business accounts;
- Content from the Instagram Community Safety Centre;
- Content from the Instagram Anti-Bullying Centre;
- The Teen Guide on Bullying;
- Content from the Instagram Parent's Centre;

²⁷⁶ FB-I's submission of 27 October 2020, paragraph 5

- The Instagram Parent’s Guide;
- Copies of the account switching process (before and after September 2019);and
- Copies of the account creation process.

326.FB-I submits²⁷⁷ that it put in place staff to monitor safety issues, as follows:

“In addition to the safety, privacy, and security tools operating on-platform, Teen safety issues are reviewed and handled by hundreds of employees from numerous cross functional teams. Safety Policy, Public Policy, Product, Legal Safety & Security, and Integrity teams, among others, have employees dedicated exclusively to Teen safety. These employees utilise their subject matter expertise to understand existing and emerging issues related to Teen safety and privacy on Instagram, work with nonprofits to develop Teen-appropriate policies, and advocate for and develop improvements in products and procedures within the company.

327.While the existence of cross-functional safety teams and information resources may be relevant measures and safeguards in the context of Articles 24 and 25 GDPR, the effectiveness of these measures must be assessed with regard to the specific processing operations at issue.

328.In its submission of 9 August 2021, FB-I indicated that it had also implemented specific measures to mitigate the risk that communication between a dangerous person and a child user could be taken off-platform. In this regard, FB-I stated as follows²⁷⁸:

“To address potential risks of grooming, child trafficking, and child exploitation, Facebook Ireland and its processor, [Meta Platforms, Inc.] have focused efforts in particular in the following areas for well over a decade to develop policies, safety programs, and educational resources with more than 400 organisations around the world to help make the internet a safer place for children:

- a) **NCMEC partnership.** Facebook partners closely with the National Center for Missing and Exploited Children (NCMEC) in reporting instances of child exploitation from around the world. NCMEC coordinates with the International Centre for Missing and Exploited Children (ICMEC) and law enforcement authorities from around the world including the Irish Gardaí.
- b) **Child Safety Hackathon.** Facebook hosts a child safety-dedicated hackathon to bring together engineers and data scientists from across the industry to develop technological solutions to help combat child sex trafficking. For example, the winning prototype at one of its recent hackathons makes use of clustering analysis and information that is

²⁷⁷ FB-I’s submission of 18 December 2020, paragraph 3

²⁷⁸ FB-I’s submission of 9 August 2021, paragraph 98

associated with known child sex traffickers to help ensure that these individuals are not able to resurface elsewhere on the internet. All code and prototypes developed for these hackathons are donated back to the Technology Coalition and Facebook's NGO partners to help them in their work to protect kids.

- c) **Internet Watch Foundation funding.** *Facebook recently committed to help fund the Internet Watch Foundation's initiative for young people to confidentially report self-generated sexual images of minors, and to help fund a project led by Tech Matters that will develop new technology to support child helplines and make them more accessible to children in crises.*
- d) **Project Protect.** *Recognising that child exploitation is a problem across the internet and it is a collective responsibility to fight this abuse and protect kids online, Facebook recently joined Google, Microsoft, and 15 other tech companies to form Project Protect, a plan to combat online child sexual abuse. Project Protect focuses on five key areas: (1) Tech Innovation: to accelerate the development and usage of groundbreaking technology powered by a multi-million dollar innovation fund; (2) Collective Action: to convene tech companies, governments, and civil society to create a holistic approach to tackle this issue; (3) Independent Research: to fund research with the End Violence Against Children Partnership to advance a collective understanding of the patterns of child sexual exploitation and abuse online; (4) Information and Knowledge Sharing: to continue to facilitate high-impact information and expertise; and (5) Transparency and Accountability: to increase accountability and consistency across industry through meaningful reporting, in conjunction with WePROTECT Global Alliance."*

329. With regard to the above measures, I note the following:

- The above four measures all relate to the prevention and detection of online child exploitation and abuse. While FB-I has not provided much detail on the measures at issue, it is possible that FB-I's involvement in the above initiatives may well contribute to the objective of child safety online.
- The above measures have a primary focus on retrospective steps to protect children who have already been affected by online exploitation and abuse. The measures include important safeguards and corrective measures in the field of child protection. However, such measures are focussed primarily on the point of crisis, where a child may have already been severely affected by exploitation and abuse.

- As is clear from the NSPCC statistics on the UK offence of sexual communication with a child (described further at paragraph 274 above), instances of child abuse and exploitation on the Instagram platform may become known to FB-I as a result of criminal investigations. While it is essential that FB-I respond appropriately to requests by law enforcement agencies, such reporting activities of themselves may do little to mitigate or reduce the causes of risk to children.
- The clustering project referred to by FB-I in relation to the Child Safety Hackathon is described in a contemporaneous press release from Facebook²⁷⁹ as a “*prototype*”. It is unclear whether the prototype in question has been implemented with regard to FB-I’s processing, or otherwise. FB-I has not explained whether or how this prototype, or other prototypes from the Hackathon, are implemented in practice with regard to the processing at issue.
- Although FB-I states that it has engaged with more than 400 bodies over the course of a decade, two of the specific examples provided are said to have occurred “recently”, without further information. For example, Project Protect was announced on 10 June 2020²⁸⁰, and therefore may be of reduced relevance to this Inquiry, which concerns processing of personal data before that time.

In conclusion, FB-I is to be commended for its involvement with these initiatives, which can mitigate the damage caused to children as a result of online abuse and exploitation. However, the above initiatives alone would not be sufficient to meet FB-I’s obligations under Articles 24 and 25 GDPR with regard to the two types of processing at issue. In particular, these measures appear to be focussed primarily on mitigation of harm where exploitation or abuse has already taken place, as opposed to prior risk mitigation regarding the specific processing operations at issue. In other respects, the above measures appear to be at a preliminary stage of development, and refer to prototype initiatives.

330. In its submission of 9 August 2021²⁸¹, FB-I also identified additional technical measures it implements with regard to unauthorised scraping of information, as follows:

“Using automation to get data from Instagram without its permission is a violation of the Terms of Use. Dedicated functions have focused on both building systems and infrastructure to stop this type of data misuse and enforcing against entities or individuals engaged in such misuse. In short, Facebook Ireland aims to make it harder

²⁷⁹ Using Technical Solutions to Keep Children Safe, Facebook, May 24 2018, available online at: <https://about.fb.com/news/2018/05/keeping-children-safe/>

²⁸⁰ “A Plan to Combat Online Child Sexual Abuse”, Technology Coalition, Posted on: 10th June, 2020, available online at <https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/>

²⁸¹ FB-I’s submission of 9 August 2021, paragraph 98

for scrapers to acquire data from its services in the first place and harder to capitalise from it if they do. For example, this work:

- a) makes unauthorised scraping harder and less attractive to scrapers by implementing technical mitigations against scraping such as:
 - i. Rate limits, which cap the number of times anyone can interact with Facebook Products – including Instagram – in a given amount of time;*
 - ii. Data limits, which keep people from getting more data than they should need to use these products normally;*
 - iii. Request blocking through pattern recognition; the team looks for patterns in activity and behaviour that are typically associated with automated computer activity in order to block them automatically.**
- b) investigates suspected scrapers to learn more about what they are doing and use that information to make its systems stronger.*
- c) takes a variety of enforcement actions against external data misuse, including sending cease and desist letters, disabling accounts, filing lawsuits against scrapers engaging in egregious behavior, and requesting companies that host scraped data to take them down.*
- d) aims to address improperly collected data from being shared by scrapers online by engaging with threat intelligence researchers to look for examples of these datasets being shared and working with responsible hosting vendors to get them taken offline.*

The measurement, detection, and response functions identify active scraping threats and take action using technical enforcement mechanisms.

- a) Measurement: they build systems to identify where scraping may be occurring, which accounts are scraping, and the risk posed by different scraping attacks.*
- b) Detection: they build scaled defense systems that can identify and take action against scraping accounts in real time across Facebook and Instagram. Its systems constantly monitor for signs of scraping behavior and flag accounts that are deemed to be scraping so that they can be remediated by response systems.*
- c) Response: they build systems that intervene against accounts identified by the detection function. These systems manage account-related disables*

and also help users recover access to accounts that malicious actors have compromised.”

331. With regard to the above measures, the DPC accepts that FB-I has implemented certain measures to reduce the risk of unauthorised scraping of personal data in the context of the Instagram platform. At the same time, I note that Facebook has (in the context of the separate Facebook social media network) stated²⁸² that it cannot fully mitigate the risk of scraping, as follows:

“Because scrapers often mimic the ways that people use our products legitimately, we’ll never be able to fully prevent all scraping without harming people’s ability to use our apps and websites the way they enjoy.”

332. The extent to which scraping of public information can evade detection in practice was demonstrated in this case by Mr Stier’s collection of information for the purpose of submitting his report to the Facebook security team. By accessing information publicly accessible on Instagram (including in the HTML source code of profile webpages) Mr Stier indicates that he was able to analyse Instagram profiles for 18000 people based in the European Union (including cohorts of users associated with particular geographic locations in Europe), as well as more than 30,000 users based in the United States of America.

333. I am therefore of the view that although the measures implemented by FB-I to prevent unauthorised scraping may have been effective in preventing some forms of unauthorised collection of personal data, in other respects, such measures would not have prevented the targeted collection of personal data of thousands of linked Instagram users (as demonstrated by Mr Stier and notified to FB-I in Appendix 3 to the Notice of Commencement at the outset of this Inquiry).

334. With regard to the measures set out in paragraphs 328 and 315 above, FB-I states that it has raised the above child safety measures at this later stage of the Inquiry because it was *“never provided the opportunity to provide the Commission with information about its safeguards to curb any off-platform risks because it was never asked about those or made aware they were relevant to the Inquiry”*. FB-I also contends that until the PDD, it did not know that measures to prevent unauthorised scraping were *“relevant to the Commission’s considerations”*. FB-I is demonstrably incorrect in this regard. FB-I has been at liberty throughout this Inquiry to provide the DPC with all or any relevant information concerning its compliance with Articles 24 and 25 GDPR in relation to the processing at issue.

²⁸² “What is data scraping and what can I do to protect my information on Facebook?” Facebook Help Center, available online at <https://www.facebook.com/help/463983701520800>

335. There is no basis to support FB-I's contention that it was not sufficiently on notice prior to the PDD that the above risks and measures would be relevant to the Inquiry, for the following reasons:

- The notice of commencement of Inquiry expressly stated²⁸³ that FB-I's compliance with Articles 24, 25 and 35 GDPR in connection with "*The automatic setting of Child Users' (regular) Instagram profiles to public by default*" and "*The display of Child Users' phone numbers and/or email addresses in full on Instagram business account profiles*" were relevant matters. These provisions in turn refer expressly to risks associated with this processing of personal data. FB-I was therefore aware from the outset of the Inquiry that it should account for all relevant risks pertaining to the processing.
- Unauthorised scraping of public data is a widely acknowledged risk associated with public information on social networks. FB-I maintains a specific help page²⁸⁴ regarding the risk of scraping (in the context of the Facebook social media network), which states: "*Because scrapers often target data that is public, it's important to make sure that your Facebook settings align with what you want to share publicly*". FB's assertion that scraping was not a reasonably foreseeable aspect of the risks associated with the contact information processing is therefore not tenable.
- The risk of possible unauthorised scraping of personal data was also specifically raised in Mr Stier's report to Facebook on 22 February 2019. In this report, Mr Stier stated that the contact information published in the HTML source code for users was at that time "*hiding in plain sight*", with the consequence that "*virtually anyone could scrape this information for tens of millions of users*". The notice of commencement cites this correspondence between Mr Stier and FB-I, as part of the factual background to this Inquiry.
- The risk of communication between child users and dangerous individuals is also inherent to the processing at issue, and has been obvious since the commencement of the Inquiry. Indeed, FB-I itself describes the risk of communication between a dangerous individuals and child users on Instagram in part 4.2.a of FB-I's "*Legitimate Interests Assessment ('LIA') Processing minors' data for the provision of the Facebook Products*"²⁸⁵. I note that the earliest version of this LIA provided to the DPC is dated 23 October 2020 (i.e. before FB-I's first submission to the DPC in this Inquiry). In particular, the LIA at this time identified a relevant risk that a "*...minor may communicate with (and potentially develop a*

²⁸³ Notice of Commencement, Page 6

²⁸⁴ "What is data scraping and what can I do to protect my information on Facebook?" available online at <https://www.facebook.com/help/463983701520800>

²⁸⁵ Appendix H to FB-I's submission of 27 October 2020

relationship with) individual(s) who may pose a danger to that minor (e.g. grooming; physical, sexual and emotional abuse; trafficking; etc) and the minor may not be able to identify that danger”. There is accordingly no basis for FB-I to assert that this risk only became relevant following the PDD.

- Notwithstanding the obvious relevance (from the outset of this Inquiry) of the risk of unauthorised scraping of personal data, and the risk of child exploitation, FB-I maintains that the DPC ought to have specifically notified it prior to the PDD that these risks are relevant to this Inquiry. Having been asked to account for its compliance with Articles 24 and 25 GDPR at the outset of this Inquiry, FB-I’s response to the Statement of Issues identified two risks of purportedly “low” likelihood and severity which it considered to be relevant to this processing; FB-I in particular stated that “(1) *Teens may not understand how their personal data is being processed, and (2) information provided by Teens could be misused by individuals*²⁸⁶”. In its submissions in response to the DPC statement of issues, FB-I repeatedly stated²⁸⁷ that it “...is not immediately clear to Facebook Ireland from the Statement of Issues which specific risks the Commission is concerned about, given both functionalities operate within a safety-focused Instagram Service”. FB-I has nevertheless made extensive submissions concerning the risks identified in the PDD, which have been assessed by the DPC in the context of finalising this Decision. It is therefore the case that FB-I availed of an open-ended opportunity to provide information to the DPC on measures and safeguards it applies to manage processing risk.
- I am therefore of the view that the risk of child exploitation and abuse, as well as the risk of unauthorised scraping of personal data, were each manifestly relevant to this Inquiry from the outset. Notwithstanding this, FB-I elected not to address these risks in its initial submissions to the DPC, instead adopting the position that only two, general, “low” risks applied to the processing at issue, which in FB-I’s view had been adequately mitigated. It was open to FB-I to make more specific responses to the Notice of Commencement and the Statement of Issues, but it did not avail of these opportunities, for the apparent reason that it does not accept the existence of wider risks resulting from the processing at issue. I am therefore satisfied that the relevance of the above risks to this Inquiry was not remote or obscure at the outset; these risks could have been addressed by the controller itself in its initial submissions.
- The PDD contained the DPC’s preliminary views on the detailed application of the GDPR to the facts of this case. In preparing this document, the DPC had regard to all relevant materials and submissions of the controller. In circumstances where

²⁸⁶ FB-I’s submission of 27 October 2020, paragraphs 32 and 67

²⁸⁷ FB-I’s submission of 18 December 2020, paragraphs 5 and 46

the DPC did not agree with FB-I's assessment of risk (as set out by FB-I itself in its submission of 27 October 2020), the PDD described in clear terms the risks which, in the view of the DPC, actually relate to the processing at issue. Subsequent to this assessment in the PDD, FB-I has been allowed to make additional procedural, legal and factual submissions it wished to make in response to the PDD, including the Berglas Report, which was provided by FB-I after the for deadline submissions in response to the PDD had elapsed. I am satisfied that, notwithstanding the fact that FB-I decided to make detailed additional submissions in response to the DPC, I have carefully considered all such submissions made at this stage of the Inquiry.

336. On the basis of the matters set out in Paragraph 335 above, I am satisfied that FB-I was provided with ample opportunities prior to the PDD to address all relevant risks. I am also satisfied that the additional submission made by FB-I subsequent to the PDD have also been taken into account for the purpose of preparing this Decision. I am therefore satisfied that no procedural prejudice arises in the manner alleged by the controller, and additional rounds of submissions are not necessary prior to the completion of this Decision.

Measures and safeguards concerning the publication of contact information of child users

337. In its submission of 27 October 2020, FB-I made clear that the requirement/facility for child users to publish their phone and/or email contact information was an intentional step, designed to encourage the “businesses” and “initiatives” of child users, as follows²⁸⁸:

“Indeed, if Teens could not display the contact details of their businesses, particularly in the context of a service aimed at providing an environment where it is safe to do so, they would be unduly deprived of an important entrepreneurial tool to provide users with full and complete information about the business or initiative in question, and prevent users from meaningfully engaging with the business or initiative, to the detriment of both users and the Business Account owner.

...Business Accounts are appropriate for Teens because they are subject to the safety, privacy, and security features and safeguards that apply platform-wide, and were built also with Teens in mind. As set out above in further detail, the platform includes tools to block unwanted interactions and reporting channels for important issues like abuse, bullying, harassment, and impersonation. Instagram also has robust content policies, reviewing processes, proactive detection, and product interventions that are all meant to keep Teens safe across the platform – including those Teens who choose to convert to a Business Account.

²⁸⁸ FB-I's submission of 27 October 2020, paragraphs 59 and 61

338. The publication of contact information of child users did not take place solely “*in the context of*” the Instagram service and its safety features; processing in this case was global in its extent, and included publication of contact information to persons off-Instagram. Once contact information was published, Instagram had no effective control over who could access this information, or what they might do with it. In particular, FB-I made contact information of child users available for unauthorised collection by persons scraping HTML profile pages. The on-platform safety measures would not have effectively mitigated the risk of off-Instagram communication, as made possible by the publication of phone or email contact information. At the same time, the anti-scraping measures, and other off-platform measures described at paragraph 328 above would not have *proactively* mitigated the severe possible risks associated with the publication of personal contact information of children; these measures appear to mitigate risks by detecting unauthorised scraping of information which has already been published, and by taking steps to address exploitation and abuse which has already happened. Accordingly, I do not accept FB-I’s submission that publication of phone and email contact information was subject to appropriate measures and safeguards, because the measures implemented pertain almost exclusively to on-platform activities of users, and would have limited effectiveness in proactively mitigating risk.

339. FB-I submits²⁸⁹ that it intentionally excepted child users from promotional campaigns concerning business accounts, as follows:

...As explained above, Facebook Ireland notes that while the Business Account is available to Teens (by visiting their settings and completing the account conversion user flow), Teens are excluded from any promotions for switching to Business Accounts, to further ensure any such decision by a Teen is a deliberate one, taken freely and uninfluenced, mindful that Teens might be more susceptible to promotions than adult users.”

340. While I accept that the above safeguard mitigated (to an extent) the risk of child users switching to business accounts and consequently publishing their contact information by mistake, I also note that child users could nevertheless easily find the business account/professional account switching process, as it was displayed at a high level in the application settings. The button to commence this process was prominently situated and would have been obvious to all users on a cursory review of the Instagram application settings. I am also of the view, as addressed above at paragraph 248, that the free “*insights*” provided by FB-I to business account users would quickly come to the attention of child users and their peers. The additional information provided to business account users about their followers could foreseeably have acted as an incentive for switching to a business account, even where the child user had no intended professional purpose. It is not clear that the above measure was sufficient to ensure that only well-informed child

²⁸⁹ FB-I’s submission of 27 October 2020, paragraph 60

users with a professional purpose would switch account, because the switching process was easily accessible, incentivised by free additional features, and streamlined to ensure rapid and seamless switching between account types.

341. FB-I also submits, in the context of safeguards and the use of business accounts by child users, that it provided relevant information in relation to online safety, as follows²⁹⁰:

“For example, Facebook Ireland publishes information for Teens so they can learn about all tools available on Instagram and tips on how to stay safe online. Facebook Ireland also offers a dedicated online Parent Centre and has published a Parent’s Guide with information about Instagram and its privacy and safety tools, top questions for parents, and talking to their Teen about staying safe on Instagram.”

342. Having considered the information provided by FB-I to child users and parents, it is notable that no information was provided to users regarding the risks of publishing their personal contact information, nor did the Parents’ Guide explain to any extent that publication of contact information of child users may be required/facilitated in the context of business accounts. It appears that the safety information provided by FB-I to child users of Instagram is directed towards on-platform safety and privacy issues (such as anti-bullying measures), and neglects to warn child users with regard to the risks posed by off-platform publication of contact information, and subsequent communication between child users and dangerous individuals (as well as other risks specified above). I acknowledge that the GDPR does not require a specific warning as to adverse consequences the context of Article 24 or 25; my observation as to the lack of timely information in this respect goes to the quality and extent of measures and safeguards implemented by FB-I. Accordingly, I am not satisfied that the information provided by FB-I acted as an effective safeguard to protect the rights of data subjects in connection with the publication of child users’ phone and email contact information.

343. FB-I contends that the account switching process itself was a safeguard, because it was purportedly drafted and presented in such a way that only well-informed users with a professional purpose would avail of this option, as follows:

“With respect to safeguards applicable to Business Accounts, in particular, as explained above, the means for converting a personal account to a Business Account requires that a user specifically seek out to convert his or her personal account and then complete a dedicated flow that provides transparency and information in relation, in particular, to the display of a contact option. The user flow is presented with a simple user interface (in keeping with the Instagram aesthetic), which makes for effective delivery of information to both Teens and adults (...) As relevant to the Inquiry, the current user flow has two dedicated screens explaining that the user may

²⁹⁰ FB-I’s submission of 27 October 2020, paragraph 62

choose to display a contact option. The final page of the flow also includes a prominent button labelled “Don’t Use My Contact Info”.

344. The scope of this Inquiry includes an assessment of processing by FB-I prior to the changes to the business account process as of 4 September 2019. In this regard, I note that the *“Don’t Use My Contact Info”* opt-out button was not provided to users prior to September 2019, because at that time FB-I required the provision of either a phone number or an email address by business account users (including child users aged 13), as an essential prerequisite to switching account. It also appears that FB-I has not directly notified pre-September 2019 business account users of the change in its contact information policy, as discussed in part F.3 above in relation to Finding 4. I also note that the *“simple user interface”* employed for the switching process is not a safeguard, because by streamlining the switching process (and auto-filling contact information using personal data obtained during registration) FB-I increased the risk that a child user would move through the process without considering its content and the risks arising. In particular, I note that the design language employed by FB-I, whereby each option screen contained a single large blue button to progress to the next screen (resulting in the publication of the user’s auto-completed contact information). This design approach made it easier for child users to simply ignore the information content of the switching process. I also note that both versions of the switching process neglected to advise users of the risks associated with publication of personal contact information to persons off Instagram. In conclusion, I am satisfied that the business account switching process increased the risk that child users would inadvertently or inappropriately publish their personal contact information, and I am satisfied that the processes used did not contain sufficient safeguards to protect the rights of child users in the context of the contact information processing.

345. I have also considered whether modifications of FB-I’s contact information processing can be regarded as appropriate and effective measures and safeguards. In this regard, I note that FB-I removed phone numbers and email addresses from the HTML source code for a time between March 2019 and August 2020. FB-I reintroduced the HTML contact information in August 2020, only to cease processing this information again in or around November 2020. I accept that the removal of the information from the HTML source code was an effective measure and safeguard, albeit a measure which was intermittently applied, and disregarded without notice in August 2020.

346. I have considered whether FB-I’s decision to split the *“business account”* into two forms of professional account (*“creator accounts”* and *“business accounts”*) in July 2019 was a relevant measure and safeguard for the purpose of the GDPR. I accept that individual child users are now more likely to be offered a creator account than a business account, thereby reducing the likelihood of inadvertent disclosure of personal contact information. Notwithstanding this, it remained possible for a child user to select a

business account instead of a creator account during the switching process. Where a child user selected a business account instead of a creator account after July 2019, FB-I populated the contact information fields in the switching process with existing contact information obtained during the user's registration for a personal account. This would have resulted in a rapid and streamlined account switching process, which did not include a specific warning to the child user regarding the risks or possible adverse consequences of publishing their contact information.

347. Finally, I have considered whether the contact information opt-out implemented by FB-I in September 2019 was a relevant measure and/or safeguard for the purpose of the GDPR. In this regard, I accept that the introduction of this opt-out reduced the likelihood of unwanted or inappropriate publication of contact information of child users who switched to a business account after that time. However, I also note that FB-I populates the contact information fields in the switching process with existing contact information obtained during the user's initial registration. This results in a rapid and streamlined account switching process, which does not include any specific warning to the child user regarding the risks and possible adverse consequences of publishing contact information. I also note that FB-I has not directly notified persons who switched accounts prior to September 2019 that contact information publication is no longer a requirement (as discussed above in Part F.3 above in connection with the fourth transparency issue).

348. In summary, the changes set out above in paragraphs 345 to 347 all tend to decrease the risk that contact information of child users would be published inadvertently and inappropriately. Notwithstanding this, the processing of contact information of child users (as of 22 February when Mr Stier first contacted Facebook) was clearly high-risk processing with severe possible consequences. Subsequent changes have been implemented in a staggered, intermittent manner, and one of the measures (in the case of HTML content) has been rolled back for a time without notice to users. It is also the case that, despite changes since July 2019, the account switching processing continues to facilitate child users' publication of email and phone numbers, in a process that lacks specific and targeted warnings of the severe risks associated with loss of control over personal contact information. The automatic population of contact information also streamlines the switching process. This increases the risk that younger child users (who may be less aware of the risks, consequences and safeguards of processing) may inadvertently or inappropriately disclose sensitive personal information in the form of their off-Instagram contact details.

Measures and safeguards regarding the public-by-default audience setting

349. In its submission of 27 October 2020, FB-I stated that it took steps to ensure that only persons over the age of 13 were allowed to register as Instagram users²⁹¹. FB-I also stated²⁹² that it provides on-platform safety measures (including anti-bullying measures), and information on platform safety and privacy. FB-I submitted that these measures and safeguards were in compliance with its *“obligations to Teens under Articles 24 and 25 and accordance with Recitals 38, 75, and 76 GDPR”* in connection with the public-by-default processing of social media content.
350. In its response to the Statement of Issues, FB-I made a number of submissions regarding the adequacy of the measures it implements to protect the rights and freedoms of child users on the Instagram platform, with regard to the public-by-default processing of social media content of child users.
351. FB-I submitted that it is appropriate to implement *reactive* safety and privacy tools, and settings which require *proactive* steps by child users, on the basis that the inherent purpose of Instagram, and the expectation of child users, is that content will be shared with others. FB-I contends²⁹³ that *“[p]roviding settings that require a degree of proactivity on the part of the User to move away from sharing with others by default is consistent with Users’ expectations, as they join Instagram for this purpose”*. I do not agree that all users can be regarded as having a single intended purpose for how they will use Instagram, for the reasons discussed above at paragraph 250 onwards. It is equally valid to say that many users wish to share their content only with people they know; this alternative purpose of the Instagram service was clearly reflected by the “private” audience setting implemented by FB-I.
352. FB-I further submits²⁹⁴ in this regard that the DPC has *“focussed too singularly”* on the default public setting, without acknowledging that child users may also experience bullying by their approved followers, and conversely, could receive *“positive connection and support”* from a wider audience of users. FB-I contends that it has created adequate, context-specific protections for both modes of using Instagram, and submits that it is an *“oversimplification to suggest that narrower audience settings means a more protected experience”*. I do not accept FB-I’s submission in this regard, which draws a false equivalence between private and public accounts; both types of account pose a risk of bullying for child users, but only public accounts expose child users’ social media content to an indeterminate global audience of strangers. It is not an *“oversimplification”* to recognise that a child user who posts content in a public account has a less protected experience, because the element of personal control is absent by default, and the potential consequences of sharing are less predictable for the user. The risk associated

²⁹¹ FB-I’s submission of 27 October 2020, paragraphs 50 and 51

²⁹² FB-I’s submission of 27 October 2020, paragraphs 52 to 55

²⁹³ FB-I’s submission of 18 December 2020, paragraph 22

²⁹⁴ FB-I’s submission of 18 December 2020, paragraph 23

with large-scale processing of social media content (which is an inherent feature of public-by-default accounts) is specifically acknowledged in Recital 75 GDPR. By “nudging” child users into a public-by-default audience setting prior to 2021, FB-I prioritised its aim of wider engagement between Instagram users, while requiring proactive steps on the part of the user to obtain a more private experience.

353. FB-I contends²⁹⁵ that *“certain features, by their very nature, require proactivity from users in order to empower them to best control their experience on the Service. In particular blocking tools are, by necessity, reactive, as it is the User who is best placed to determine who they would like to block”*. It is not my view that reactive user controls are inadequate in all circumstances. However, reactive blocking tools such as those implemented by FB-I are less effective in circumstances where a user may have already suffered serious negative consequences before they can exercise the controls provided. The adequacy and effectiveness of reactive blocking and reporting tools depends to a large extent on the severity and likelihood of the corresponding risk posed to the user. For example, blocking and reporting tools do not appear to be effective measures in cases where someone sends a child sexually explicit material via direct message on Instagram, or uses the direct message feature to persuade a child to communicate off-Instagram. In its submission of 9 August 2021²⁹⁶, FB-I states that the DPC *“appears to go so far as to suggest that the existence of part of the Service – the direct message functionality – should be eliminated for Teen Users or at least very significantly restricted; or that Facebook Ireland should be monitoring the content of private user messages, a measure that would raise difficult questions in relation to message privacy, which the PDD does not address”*. This is not correct; the DPC has assessed the concrete measures implemented by FB-I in the context of its compliance with the GDPR; however, the DPC has not in this instance suggested that the processing in question should be monitored or eliminated. It is possible that alternative steps could be taken by FB-I to mitigate the risks in question. It is FB-I’s responsibility as controller to identify and implement such measures.

354. In its submission of 9 August 2021²⁹⁷, FB-I submits

“The Commission’s analysis also appears to be premised on what Facebook Ireland submits is an incorrect conclusion that sharing photos and videos publicly directly and inevitably leads to the on and/or off-platform communications which the Commission relies upon. It does not, and as a result Facebook Ireland submits that the PDD overstates the potential risks. First, this analysis does not take account of the safeguards that have been implemented to mitigate such off-platform harms. Secondly, a non-user viewing any content on a public Instagram account would, for

²⁹⁵ FB-I’s submission of 18 December 2020, paragraph 24

²⁹⁶ FB-I’s submission of 9 August 2021, paragraph 101

²⁹⁷ FB-I’s submission of 9 August 2021, paragraph 105

example, still need to create an Instagram account in order to direct message the user who posted such content so as to initiate contact – meaning that the full suite of on-platform measures and safeguards that Facebook Ireland has implemented would apply.”

I do not agree with the above statement by FB-I. The DPC is not of the view that communication between child users and dangerous individuals is inevitable. However, the consequences of such communications, when they occur, may be severe. The DPC is therefore in agreement with FB-I’s own assessment of risk as set out in the LIAs; communication between dangerous individuals and children is a risk, the likelihood of that risk is “possible”, and the potential consequences associated with the risk are severe. The DPC’s assessment of measures and safeguards in this regard is therefore not premised on an exaggerated view of the pertinent risks, and off-platform mitigation measures, as set out in detail above. Further to this, FB-I’s view that dangerous individuals would always need to set up an Instagram account in order to contact a child is not accurate in every case. In particular, where FB-I has required/facilitated the publication of a child’s contact information, a person could contact that child directly, without the need to register as an Instagram user. Further to this, and as pointed out in the Berglas Report, dangerous individuals may mask their location or IP address by using a virtual private network, and therefore, efforts to identify the true identity of persons on the Instagram platform may not be effective.

355.FB-I contends²⁹⁸ that it is “*not accurate to say that the measures implemented by Facebook Ireland to keep Users, including Teen Users, safe on the Service all require proactivity from the User. Technologies such as media matching and machine learning classifiers are important examples to the contrary*”. I have considered the adequacy of these tools as measures and safeguards in the context of the processing at issue. In this regard, I note that media matching depends on comparative assessment of existing media, which may not detect original explicit material sent to a child user. I further note that FB-I’s implementation of machine learning classifiers on Instagram does not appear to include automated assessment of the content of direct messages, which are “private” between the sender and the receiving user. This apparent fact was outlined by FB-I in a blog on 10 February 2021²⁹⁹, which stated:

*“The abuse we’re seeing is happening a lot in people’s Direct Messages (DMs), which is harder to address than comments on Instagram. Because DMs are for private conversations, **we don’t use technology to proactively detect content like hate speech or bullying the same way we do in other places.** But there are still more steps we can take to help prevent this type of behavior. So today we’re announcing some*

²⁹⁸ FB-I’s submission of 18 December 2020, paragraph 25

²⁹⁹ <https://about.instagram.com/blog/announcements/an-update-on-our-work-to-tackle-abuse-on-instagram>

new measures, including removing the accounts of people who send abusive messages, and developing new controls to help reduce the abuse people see in their DMs.” (emphasis added)

356. It therefore appears that media matching and machine learning classifiers (as implemented by FB-I) are not effective means by which to detect abusive communications sent to child users by direct messages on Instagram. It is also the case that these techniques would not be effective in respect of off-Instagram communication.

357. With regard to information provided to child users, FB-I submits³⁰⁰

“...where tools and features do require Users to take proactive steps, Facebook Ireland appropriately informs and educates Users -- especially Teens -- about how they can find and utilise them. This includes, for example, the Teen- and Parent-oriented educational materials discussed in the First Submission. And Facebook Ireland also proactively notifies Teens about new and upcoming features designed to protect them. For example, when Facebook Ireland rolled out Restrict (designed with the Teen-focused aim of preventing bullying on Instagram, as discussed in the First Submission), Facebook Ireland used in-app notifications via Users’ activity feed in order to drive adoption.

358. I have therefore considered the material provided to child users and parents by Instagram. I note that the information resources provided to child users and parents by Instagram referred to the ability to report “inappropriate” posts received by child users to Instagram. However, no express reference is made in the Community Safety Centre or the Parent’s Guide to the possibility of contact between dangerous individuals and child users, which may result in *“grooming; physical, sexual and emotional abuse; [or] trafficking”*³⁰¹ and severe impacts for the rights of child users, nor is any mention made of the risks of off-Instagram communication. I am therefore satisfied that the information and education resources did not effectively safeguard the rights of child users, on the basis that insufficient information was provided concerning the risks associated with the specific processing at issue (i.e. global visibility of child users’ social media posts by default).

359. In its submission of 9 August 2021, FB-I reiterated its position that the on-platform controls provided to child users were effective and appropriate measures. These measures have been addressed above. FB-I further contended³⁰² that the audience setting itself was a relevant measure for the purpose of Articles 24 and 25 GDPR, insofar that it allows users control over the visibility of their personal data. In making this submission, FB-I also maintained that the audience setting also takes into account other

³⁰⁰ FB-I’s submission of 18 December 2020, paragraph 26

³⁰¹ Risks cited in FB-I’s Legitimate Interests Assessment of 23 October 2020, section 4.2.a

³⁰² FB-I’s submission of 9 August 2021, paragraph 104

rights and freedoms of users (presumably in the form of the users' freedom of expression. FB-I did not acknowledge that the audience setting may mitigate the risk of communication between child users and dangerous people.

360. While FB-I is correct insofar that the audience setting allows the user to control the extent of processing on Instagram, this measure must be assessed in its full context. At the relevant time periods under consideration, FB-I elected not to bring this measure to the attention of child users at the point of registration. This had the effect of “nudging” child users into a public account by default. Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. In particular, there was a risk that child users may not understand the audience setting; this is borne out for example in a 2017 survey Bulgarian child users³⁰³, which found that one in four of the children surveyed were not “*confident in their ability to change the privacy settings of their profiles*”. It is therefore difficult to attach significant weight to this measure in the context of FB-I’s public-by-default processing, because the measure was not brought to the attention of child users at the point of registration, and because a more extensive form of processing (i.e. a public account), with less control for the user over the audience for social media content, was implemented by FB-I as a default setting.

Conclusion regarding measures and safeguards

361. With regard to the assessment of measures in the context of Articles 24 and 25, FB-I contends that the DPC should give greater weight to the potential benefits of social media use to child users. In this regard, FB-I states³⁰⁴:

“...the Commission should give more weight in its analysis to the competing benefits of Teens utilising services that foster free expression, community, and sharing in the manner the functionalities under consideration did. This (when coupled with appropriate mitigations such as those implemented by Facebook Ireland) outweighs the potential risks identified by the Commission -- particularly where potential risks of this nature are inherent in the online and offline activities Teens take part in.”

As I have stated above at paragraph 125, I am in agreement with FB-I that the rights and freedoms of child users may be adversely impacted should they be “locked out” of elements of online services, or provided with a less complete service in comparison to adult users, in a disproportionate manner. Such an approach risks interfering with the child’s right to express their views fully, their right to freedom of expression and to seek, review and impart information and ideas. At the same time, it is not evident in the circumstances of this case that FB-I was forced to choose

³⁰³ Are Digital Natives Digitally Literate? Insights from a national representative survey (authors: Petar Kanchev, Marko Hajdinjak, Emanuil Georgiev and Georgi Apostolov, Bulgarian Safer Internet Centre; 2017)

³⁰⁴ FB-I’s submission of 9 August 2021, paragraph 106

between effective and appropriate risk mitigation measures on the one part, and ensuring the rights and freedoms of children on the other. It is possible to operate a professional profile without also publishing contact information, and it is possible to engage freely with others on a social network without also having a public profile by default. In short, risk mitigation and freedom of expression are not always “*competing*” benefits; it is possible to accommodate both of these objectives by implementing appropriate safeguards and measures.

362. Having considered the measures and safeguards described by FB-I which were intended to ensure compliance with the GDPR and to safeguard the rights of child users, I note that FB-I has implemented certain measures and safeguards which allow child users to control their experience on the platform, for example measures which safeguard against bullying. However, I also note that the processing which is at issue in this Inquiry involves the **public and off-Instagram** dissemination of contact information of child users. Once a child’s contact information is made available in this way, the on-platform reporting tools and safeguards implemented by FB-I would be completely ineffective, because direct contact would be possible using modes of communication outside of FB-I’s control. At the same time, the effectiveness of off-platform mitigation measures, as identified by FB-I in its response to the PDD, are primarily focussed on mitigating damage to child users where processing of personal data has resulted in harm or loss of control over personal data. These off-platform measures do not effectively mitigate the risks of processing on a prior basis.

363. Further to this, the in-app tools to report abuse were ineffective to the extent that that user reporting is a reactive step that relies on the initiative of a child user. This is of particular relevance with regard to the public-by-default account setting, which exposes social media posts by child users to an indeterminate audience of Instagram users, who (as of the commencement of this Inquiry) could then contact child users confidentially using the direct message function. In particular, I note that a child user may already have received an inappropriate, dangerous or abusive communication before they can report the sender to Instagram, resulting in an unmitigated and severe impact on the child.

364. In conclusion, I am satisfied that there are possible and severe risks associated with the two forms of processing which are the subject of this Inquiry; these risks are primarily related to possible communication between child users and dangerous individuals, both on and off the Instagram platform (but also include the risk that personal data of child users could be used in the context of fraud or impersonation). I am also satisfied that the measures and safeguards implemented by FB-I (in the form of account options, tools and information) were not adequate with regard to the specific processing operations at issue, for the reasons stated above. In particular, the measures and safeguards implemented by FB-I did not adequately mitigate the risk of communication between dangerous individuals and child users. Accordingly, I do not share FB-I’s view that the

processing at issue did not result in high risks to the rights and freedoms of child users, for the purpose of Articles 24, 25 and 35 GDPR, which are addressed further in turn below.

H. Assessment of FB-I's Compliance with Article 35 GDPR

H.1 Compliance with Article 35 GDPR

365. Article 35(1) GDPR requires a controller to conduct a Data Protection Impact Assessment (hereinafter “**DPIA**”) where processing is likely to result in a high risk to the rights and freedoms of individuals, as follows:

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.”

366. Article 35(7) GDPR provides:

“The [DPIA] shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

and

...

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.”

367. The WP29 has published DPIA Guidelines³⁰⁵ on the assessment of whether processing is “high-risk” for the purposes of Article 35. The DPIA Guidelines were subsequently endorsed by the EDPB in May 2018.

368. The DPIA Guidelines recommend that in most cases, a data controller will require a DPIA when processing meets two or more of the criteria listed at pages 9-11 of the Guidelines. However, the DPIA Guidelines also state that processing which meets only one of the

³⁰⁵ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248 rev.01

nine criteria may nevertheless pose a sufficient risk so as to require a DPIA. The screening criteria for conducting a DPIA which are specified in the Guidelines are as follows:

- Evaluation or scoring;
- Automated-decision making with legal or similar significant effect;
- Systematic monitoring;
- Sensitive³⁰⁶ data or data of a highly personal nature;
- Data processed on a large scale;
- Matching or combining datasets;
- Data concerning vulnerable data subjects (including children);
- Innovative use or applying new technological or organisational solutions; and
- When the processing in itself prevents data subjects from exercising a right or using a service or a contract

369. The DPIA Guidelines also address a controller's obligation to carry out a DPIA in circumstances where processing may have commenced prior to the application of the GDPR, as follows:

*"As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed. Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations."*³⁰⁷

370. The Statement of Issues included, as matters for determination, an assessment of whether FB-I has complied with its obligations under Article 35 GDPR in respect of the processing that is described in part C.3 of this Decision. In particular, the Statement of Issues included consideration of whether FB-I failed to conduct a DPIA pursuant to Article 35 in relation to the contact information processing, and/or the public-by-default processing.

H.2 Submissions of FB-I regarding Article 35 GDPR

371. In its submissions to the DPC, FB-I initially stated that it had not carried out a DPIA under Article 35 GDPR, on the basis that it was not required to do so in the circumstances. In its submission of 9 August 2021, FB-I made an entirely different and new submission on its compliance with Article 35 GDPR; it contended that although it was not required to produce a DPIA, its Legitimate Interests Assessments otherwise met the requirements of Article 35.

³⁰⁶ The term "sensitive" in this context, as used in the DPIA guideline, includes but is not limited to Article 9 personal data

³⁰⁷ WP248 rev.01, page 14

372. In its submission to the DPC of 27 October 2020, FB-I submitted the following³⁰⁸ with regard to the contact information processing:

“Facebook Ireland has not carried out a DPIA specifically in relation to the functionality that allows Teens to switch to a Business Account because Facebook Ireland does not consider this processing satisfies the criteria under Article 35 GDPR, including because the processing is not likely to give rise to a high risk to the rights and freedoms of Teens. Nor does Facebook Ireland consider that the processing meets the criteria set down [in the DPIA Guidelines]”

373. FB-I indicated that it had identified two relevant risks pertaining to the contact information processing – *“(1) Teens may not understand how their personal data is being processed, and (2) information provided by Teens could be misused by individuals”*. FB-I contended that these risks should be categorised as *“low”*, and noted the following factors which informed its risk assessment:

“The nature and scope of the processing for a Business Account is largely the same as the processing for a normal account – the main difference being that the user may choose to display a contact option button on their Business Account. However, even if this functionality did not exist, Teen users could include contact information in the “free text” section of the personal account profile or include contact information within a post. Therefore, there is no material increase in risk in allowing Teens to choose to support their business or initiative with a contact option button.

The user flow for switching to a Business Account clearly guides the user through the process of switching, including the decision of whether, or not, to display a contact option and also makes clear that this choice may be reversed at any time; and

The processing is necessary to provide a service that gives effect to Teens’ fundamental rights to conduct a business, to express themselves, communicate, and engage with information and communicate relevant to their interests and passions, while building community and their own brands.”

374. In its response to the Statement of Issues, FB-I further stated³⁰⁹:

“...The Commission’s Statement of Issues focuses on (i) a Teen account’s default audience settings (e.g., who can see their posts and stories) and (ii) the (now optional) public display of a contact information button on the profile of Teen Users who choose to switch to a Business Account. It is not immediately clear to Facebook Ireland from the Statement of Issues which specific risks the Commission is concerned about, given both functionalities operate within a safety-focused Instagram Service.

³⁰⁸ FB-I’s submission of 27 October 2020, pages 24 and 25

³⁰⁹ FB-I’s submission of 18 December 2020, paragraphs 5 and 6

...Facebook Ireland maintains that its practices concerning both issues are carefully designed to comply with applicable data protection legislation.”

375. In response to the PDD, FB-I argued³¹⁰ that it did not consider there to be an obligation to provide granular assessments with regard to the processing at issue, and the processing at issue was otherwise not likely to result in high risks. FB-I further contended that the DPC was attempting to implement a blanket requirement for a DPIA for all processing of children’s personal data, on the basis of draft guidelines³¹¹ prepared by the DPC. The allegation regarding the implicit application of draft guidance is dealt with at paragraph 67 above.

376. In its submission of 9 August 2021³¹² FB-I asserts that the DPC has elevated “*form over substance in failing to give proper weight to the data protection risk assessment contained in Facebook Ireland’s LIA*”. Prior to this submission, FB-I had in fact never sought to rely on its LIAs as a means of compliance with Article 35 GDPR. FB-I contends that it “*undertook an assessment that satisfied the requirements of Article 35(7) GDPR in substance, albeit this was documented in the form of the LIA*”. In particular, FB-I contends that parts 2 to 5 of the LIA complied with the requirements of Article 35(7) GDPR. In conclusion, FB-I states: “*...even if an obligation arose under Article 35 GDPR in this case (which [FB-I] disputes), the Commission’s preliminary findings of infringement of Article 35 GDPR...should be considered as allegations of “technical” violations, at most (i.e., did Facebook Ireland produce a document entitled “DPIA” vs. “LIA”)*”.

377. FB-I also submits³¹³ as a “threshold matter” that the DPC assessment of risk for the purpose of Article 35 GDPR incorrectly focusses on *potential* risks, which are not put in context, and without assessing the “*true level*” of the risks. I am satisfied that in Part G of this Decision, I have adequately considered the pertinent risks, including consideration of the context of the processing, and the need to balance risk with other concerns, such as the right of freedom of expression. I also note that concrete factual documentation of risk is contained in Part G, including among other sources, the report of the NSPCC. I refer to the analysis in Part G of this Decision in this regard.

H.3 Analysis and findings of the DPC regarding Article 35

378. At the outset, I note FB-I’s general contention³¹⁴ that it has not been made aware of relevant risks that may pertain to the two forms of processing at issue. It nevertheless appears from FB-I’s LIA³¹⁵ that the controller is acutely aware of the risks that result

³¹⁰ FB-I’s submission of 9 August 2021, paragraphs 69 and 70

³¹¹ Data Protection Commission – “*Children Front and Centre - Fundamentals for a Child-Oriented Approach to Data Protection*” – Draft version published December 2020

³¹² FB-I’s submission of 9 August 2021, paragraphs 80 to 82

³¹³ Ibid, paragraph 72

³¹⁴ FB-I’s submission of 18 December 2020, paragraphs 5 and 6

³¹⁵ “Likely Impact on Individuals” section 4.2

directly from this processing. It is also clear that the risks which give rise to obligations under Article 35 have been outlined in detail since (at least) October 2017, when the WP29 published its DPIA Guidelines, and prior to that in the form of Recital 75 GDPR. Accordingly, I do not accept FB-I's submission that there is a lack of clarity as to the relevant risks for the purposes of Article 35.

379. I also note that both types of processing at issue appear to have commenced prior to the application of the GDPR in May 2018. Nevertheless, it is clear that the relevant processing operations have been under frequent review and amendment by FB-I since that time, giving rise to ongoing obligations under Article 35, as described in the DPIA Guidelines³¹⁶.

380. Article 35(1) requires a DPIA in circumstances where processing is likely to result in a high risk to the rights and freedoms of natural persons. Article 35(7) requires a controller to describe (as part of the DPIA) the *"measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data"*. Reading these two provisions together, it is clear that risk mitigation is a matter to be addressed in the context of a DPIA. The fact that high-risk processing may have been mitigated by certain measures does not allow a controller to dispense with the underlying obligation to carry out a DPIA. The purpose of a DPIA is to inform the necessary mitigation measures³¹⁷. High-risk processing remains subject to Article 35 GDPR on an ongoing basis, even where certain measures have been adopted by a controller to address the risks.

Consideration of whether either of the two LIAs prepared by FB-I also complied with Article 35 GDPR

381. I have first considered whether the Legitimate Interests Assessments (LIAs) prepared by FB-I also comply with the requirements of Article 35 GDPR. In the course of this Inquiry, FB-I provided the DPC with two versions of the LIA, titled *"Legitimate Interests Assessment ('LIA') Processing minors' data for the provision of the Facebook Products"*. The primary purpose of this document is to assess the legal and factual aspects of FB-I's compliance with Article 6(1)(f) GDPR. A version of the LIA was first provided to the DPC on 27 October 2020, as an appendix³¹⁸ to FB-I's first submission. A header on each page of this LIA states *"Last updated: 23 October 2020"*. A second version of the LIA was provided to the DPC on 29 January 2021. A header on each page of this LIA states *"Last updated: 28 January 2021"*. It therefore appears that FB-I provided the DPC with two versions of the LIA, each of which was modified in some unspecified way after the commencement of this Inquiry. The temporal scope of this Inquiry includes the period of

³¹⁶ WP248 rev.01, page 14

³¹⁷ Recital 84 GDPR states "The outcome of the [DPIA] should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation"

³¹⁸ FB-I's submission of 27 October 2020, Appendix H

time between the application of the GDPR and the commencement of the Inquiry. Although it is not clear when exactly the LIA was initially created, or when it was updated, it appears from the content of the document that it is contemporaneous to the application of the GDPR in 2018.

382. In order for the LIAs to serve as a DPIA, it must meet the requirements of Article 35 GDPR. In this regard, I note the following:

- I appreciate that FB-I's submission regarding the LIA as a means to comply with Article 35 GDPR is made without prejudice to the controller's view that the processing at issue is not *"likely to result in a high risk to the rights and freedoms of natural persons"*. At the same time, FB-I has stated in its submission of 9 August 2021 that the risks described in the LIAs are merely potential risks, and not actual risks to be taken into account for the purpose of the GDPR. The obligation to conduct a DPIA would not be triggered in circumstances where processing is not likely to result in a high risk. As is clear from part G.2 above, I am of the view that high risks do result from the processing at issue. Accordingly, I have considered whether either of the LIAs would have operated as an Article 35 assessment of these risks.
- The LIAs were prepared to document FB-I's balancing of legitimate interests against the rights and freedoms of service users. Article 35(7) states that a DPIA must include *"a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller"*, as well as *"the measures envisaged to address the risks...and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned"*. It is therefore possible to conclude that an Article 35 DPIA may involve an assessment of the legitimate interests of a controller in the context of high-risk processing.
- Article 35(2) GDPR states *"The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment"*. There is no indication from the LIAs or from FB-I's submission that the LIAs were prepared following consultation with the controller's data protection officer.
- A single DPIA may address *"a set of similar processing operations that present similar high risks"*³¹⁹. A DPIA does not have to be specific to each type of processing, nor does it have to be in a particular form, apart from as described in Article 35 itself. In the present circumstances, I note that the LIAs are focussed on

³¹⁹ Article 35(1) GDPR

“Processing minors’ data for the provision of the Facebook Products”. The products in questions are specified in the LIA as including *“Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Oculus Products (when using a Facebook account), Bonfire, Facebook Mentions, FacebookShops, Spark AR Studio, Audience Network, NPE Team apps and any other features, apps, technologies, software, products, or services offered by Facebook Ireland Limited under our Data Policy”*. Part 1 of the LIAs sets out a *“description of processing activity”*. This description of processing is very broad, encompassing processing for all of the above services in the context of general service provision to child users. The 28 January 2021 version of the LIA includes a section which expressly asks³²⁰ if a DPIA has been prepared in respect to the processing set out in the LIA. The response contained in this section states that a DPIA has been *“conducted for the [Instagram Slimmed-Down Service]”* and explains further that as *“this LIA is designed as an overarching analysis of our legitimate interests in providing the Facebook Products to minors, the various processing activities that are carried out in providing those Facebook Products are covered by their own accountability documentation”*. It therefore appears obvious that the LIA on its own face purports to be an overarching account of certain processing, and not a specific account of high-risk processing for the purpose of Article 35. Taking the above into account, I am satisfied that the LIAs do not suffice as a means to comply with Article 35 GDPR; the description of processing is not a systemic description of similar high-risk processing operations, rather, it is a general description of processing operations related to a range of different Facebook products as provided to child users.

- More specifically with regard to Article 35(7)(a) GDPR, the first of the LIAs (i.e. the version updated on 23 October 2020), states³²¹ *“[t]he following kinds of personal data are collected for the provision of the Facebook Products...Instagram - name; phone number or email address; birthday **(none are displayed)**”* (emphasis added). Accordingly, the LIA of 23 October 2020, which is the most relevant version for the purposes of this Inquiry in terms of its temporal application, contains inaccurate information on the processing operations at issue (to the extent that Instagram did publish phone and email contact information of child users at this time, in the context of business accounts). Accordingly, the 23 October 2020 version of the LIA does not comply with Article 35(7)(a) GDPR in respect of the business account processing.

³²⁰ LIA version of 28 January 2021, part 4.2.g

³²¹ Appendix H to FB-I’s submission of 27 October 2020, page 3

- Article 35(7)(d) GDPR requires that a DPIA must include the “*measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*”. Part 4(2)(b) of the LIA states that among the “*potential negative impacts*” which arise in the context of providing the Facebook Products to child users is the risk that “*A minor may communicate with (and potentially develop a relationship with) individual(s) who may pose a danger to that minor (e.g. grooming; physical, sexual and emotional abuse; trafficking; etc) and the minor may not be able to identify that danger*”. Parts 4(2)(c) sets out the safeguards implemented by FB-I to minimise this risk. These safeguards focus on on-platform safeguards such as reporting and blocking. Paragraph 98 of FB-I’s submission of 9 August 2021 describes certain off-platform measures implemented by FB-I to mitigate the risk of child exploitation and abuse, as well as the risk of unauthorised scraping of personal data, in the context of the processing at issue. However, these off-platform measures are not included in the LIA. I am therefore satisfied that the LIA at its height represents only a partial account of the measures and safeguards implemented by the controller to mitigate the relevant risks to child users. On this basis, I am further satisfied that the LIAs do not also operate as DPIAs for the purpose of Article 35 GDPR, in respect of the processing at issue.

383. In conclusion, while I accept that there are certain superficial similarities between the LIAs and a DPIA (in particular, the LIAs do provide a detailed description of risks which arise from the provision of the Instagram service to children), the LIAs do not meet the criteria set down in Article 35 GDPR, and were clearly never intended to do so.

Was a DPIA required in respect of the contact information processing?

384. I have next considered the specific processing operations at issue. The nature, scope, context and purposes of the contact information processing by FB-I are described in Parts C.3 and G.1 of this Decision.

385. With regard to the publication of phone numbers and/or email addresses of child users, I have considered FB-I’s submission of 27 October 2020, as set out above. FB-I recognises that child users may not understand how their information will be processed, and also acknowledges that contact information may be misused. FB-I contends that this processing can nevertheless be categorised as low-risk.

386. In particular, FB-I contends that it adequately explained the processing at the point of account switching. Both versions of the switching process³²² informed child users that

³²² As set out in Appendix I and J to FB-I’s submission of 27 October 2020

“people” would be able to contact them using their contact information. However, the switching process did not include a warning of possible risks which result from public dissemination of personal phone or email contact information. Older child users and/or adults may clearly appreciate the risks of making their personal contact details public. However, it is less likely that younger child users would appreciate the risks posed by publishing their personal contact information to the world at large. I therefore do not share FB-I’s view that the information provided to child users, at the time of switching, would result in a “low” level of risk for the purpose of the application of Article 35. I also note that FB-I’s submission in this regard conflates the risk assessment and measures which mitigate a risk, as discussed above at paragraph 380.

387. FB-I also submits that there is no difference (in terms of the risk posed) between the contact information processing and general social media activity, because a child user could otherwise decide to publish their phone number or email address in an Instagram post, or elsewhere in their profile description. In my view, there is no equivalence between FB-I’s practice of requiring/facilitating the publication of information in a “structured field”³²³ – (i.e. the “Review Your Contact Info” form in the account switching process), and the hypothetical risk that a child user may spontaneously decide to publish their contact information elsewhere on Instagram without prompting from FB-I. The requirement of an email address or phone number for business accounts prior to September 2019, together with the fact that FB-I populates the contact information form with existing information it holds on the user, created a much greater risk of inappropriate and inadvertent publication of contact details than would otherwise be the case. In general, people are reluctant to publish their personal contact information, unless circumstances such as the streamlined business account switching process (and the incentive of free social media analytics) create conditions which require, incentivise or facilitate this type of disclosure. Therefore, I do not agree with FB-I’s comparative risk assessment in this regard.

388. In the context of its compliance with Article 35, FB-I also submits that this processing “*is necessary to provide a service that gives effect to Teens’ fundamental rights to conduct a business, to express themselves, communicate, and engage with information and communicate relevant to their interests and passions, while building community and their own brands.*” Article 35(1) requires that the purpose of processing must be taken into account when assessing whether processing is high-risk. I note that the publication of email and/or phone contact information is (since September 2019) optional on the part of business account users, which supports the conclusion that the professional purposes served by Instagram business accounts do not depend necessarily on the user’s ability to publish their phone and email details.

³²³ This term is used by FB-I in the LIA

389. With regard to the more specific risks identified in section 4.2 of the LIA, FB-I acknowledges the risk (among others) that dangerous individuals may contact child users, resulting in severe impacts on child users. FB-I also acknowledges³²⁴ that this risk may result in off-platform communication (i.e. by direct phone or email contact between a child user and another person). The LIA concludes that such a risk is “possible” and could lead to “severe” impacts on an affected child user. This conclusion by FB-I directly contradicts its risk assessment in the submission of 27 October 2020, which characterises the same processing as resulting in a low risk.

390. In assessing whether the contact information processing by FB-I is high-risk for the purposes of Article 35, I have also had regard to the inclusion of this information in the HTML source code for profile webpages. Prior to March 2019, and again for a period after August 2020, FB-I included contact details of business account users in the HTML source code of the web-browser version of Instagram. As is clear from the technical ease with which Mr Stier was able to use HTML web scraping to obtain contact details of thousands of Instagram users, this form of publication by FB-I created a high risk that unauthorised third-parties would engage in bulk-collection of contact details (i.e. web-scraping of personal data of child users). Scraping of phone or email information of child users poses a high risk of fraud and inappropriate communication, and may result in permanent loss of control of personal data and other negative impacts. I am satisfied that such processing resulted in a high risk to the rights and freedoms of child users, therefore requiring a DPIA to be carried out.

391. In assessing whether FB-I was or is obliged to conduct a DPIA in respect of the contact information processing, I have also considered whether processing meets the risk criteria set out in the DPIA Guidelines. In this regard, I note that the processing meets the fourth criteria - “*Sensitive data or data of a highly personal nature*” - to the extent that phone and email contact details may relate to “*household and private activities (such as electronic communications whose confidentiality should be protected)*”. The processing also meets the fifth criteria of being processed on a “*large scale*”, bearing in mind the global extent of the processing. The processing further meets the seventh criteria, in that it relates to children as a category of vulnerable data subjects. On this basis, I am satisfied that the contact information processing meets the criteria for high-risk processing set out in the DPIA guidelines.

392. In its submission of 9 August 2021, FB-I contended³²⁵ that the contact information processing did not meet any of the criteria specified in the DPIA guidelines. FB-I contends that the contact information processing does not involve “*sensitive data or data of a*

³²⁴ See “Risk 1” in tables in sections 4.2.a and 4.2.b of the LIA “...This includes risks regarding communication such as inappropriate or unwanted contact, in instances such as those arising from a user choosing to display contact details or the risk that the communication could be taken off platform.”

³²⁵ FB-I’s submission of 9 August 2021, paragraph 76

highly personal nature” on the basis that phone numbers and email addresses “do not relate to private activities, they do not impact on the exercise of a fundamental right, and their violation would not seriously impact the data subject’s life. Indeed, it is worth noting that phone numbers have traditionally been published in a public phone book.” Having considered the risks associated with, and context of the processing (as set out in Part G above), I do not agree with FB-I’s contention. A mobile phone number, or an email address, allows for direct personal access to a child. Mobile phone numbers are not comparable to traditional land-line phone numbers; mobile phones have evolved to become a central device used for the organisation and conduct of private activities, not limited to making and receiving phone calls, and therefore have a highly personal quality. Accordingly, I do not accept FB-I’s submission in this regard.

393. FB-I further contends at paragraph 76 of its submission of 9 August 2021 that the contact information processing should not be considered “large scale”. In this regard, FB-I submits that the “simple numbers of individuals concerned cannot be determinative of whether processing is occurring on a “large scale,” otherwise every single processing operation would require a DPIA (which is not the intended result of Article 35 GDPR)”. In the first instance, FB-I is incorrect in its submission that a DPIA is recommended by WP29 in respect of all “large scale” processing. The DPIA guidelines state that in most cases, processing which meets at least two of the WP29 criteria would require a DPIA; the scale of the processing is one of a number of criteria which may be considered. The WP29 DPIA guidelines suggest that the scale of processing can be considered either as a specific number of persons, or as a percentage of the overall number of data subjects. In the present circumstances, I note that [REDACTED] child users currently operate business accounts in the regions where FB-I acts as controller. It is therefore possible that the “specific number” of users involved in the processing can properly be considered “large scale”. Further to this, and as notified to FB-I in the PDD, I consider that the processing should be considered as “large scale” on the basis of the “geographical extent of the processing activity”, which the WP29 DPIA guidelines include as a relevant consideration in this context. Accordingly, my view that the processing is “large scale” is not based solely on the number of users, but also on the global extent of processing. FB-I’s submission of 9 August 2021 makes no observation regarding the global extent of the processing.

394. FB-I’s submission of 9 August 2021 also contends³²⁶ that the contact information processing does not meet the “personal data of vulnerable data subjects” criteria specified in the WP29 DPIA guidelines. FB-I quotes from the DPIA guidelines to suggest that vulnerability arises primarily as a result of imbalances in the relationship between a controller and the data subject. FB-I submits that no such imbalance exists in this case, because the processing was optional in the part of the user. In my view, FB-I’s reading of

³²⁶ FB-I’s submission of 9 August 2021, paragraph 76

this criteria is unduly narrow; Recital 38 GDPR expressly recognises that children “*merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*”. Recital 75 further cites children as a vulnerable group of data subjects. The optional nature of the processing at issue does not of itself mitigate the vulnerability of child users. In particular, child users were vulnerable in this case because they may have been less aware of the risks associated with publication of phone and email contact information. Accordingly, I remain satisfied that this criteria was met in this case.

395. FB-I further submits that the DPC has adopted the position in this Inquiry that a DPIA is required in all cases of processing personal data of children. FB-I contends that Article 35 GDPR does not include this requirement. FB-I’s characterisation of the DPC’s above position is not correct. While I am of the view that child users of Instagram should be regarded as vulnerable in the context of the contact information processing (especially bearing in mind the risks to child users associated with processing) - this conclusion goes to the DPIA criteria as set out in the DPIA Guidelines. As stated above, the DPIA criteria require a DPIA where at least two criteria are met. The DPIA guidelines do not adopt the position that all processing of children’s personal data require a DPIA, and nor has the DPC in this case. Accordingly, FB-I’s submissions in this regard are inaccurate.

396. Having considered FB-I’s submissions of 9 August 2021, I remain of the view that the contact information processing meets the above three risk criteria, as set out in the DPIA guidelines.

Conclusion and Finding 5

397. Having considered the nature, scope, context and purposes of the contact information processing (as set out above in Parts C.3 and G.1 of this Decision), I am of the view that the LIA prepared by FB-I, for the most part, correctly identified the risks which arise in relation to this processing. I also note that changes to this processing in July 2019 and September 2019 (to create alternative forms of professional accounts, and to make optional the provision of contact information for a business account) reduced but did not adequately mitigate the risks for child users in connection with the processing. In particular, FB-I facilitated the publication of phone and email contact information for children as young as 13, using a streamlined account switching process which automatically completed certain information for the user, without warning child users that publication of their personal contact information may result in high risks to their rights and freedoms. Accordingly, taking into account the above, I am satisfied that the contact information processing by FB-I (both before September 2019, and after) results in high risks to the rights and freedoms of child users, for the purposes of Article 35(1) GDPR.

Finding 5

Having taken into account the nature, scope, context and purposes of the processing of child users' email addresses and phone numbers by Facebook Ireland Limited (**as described in Part C.3 and G of this Decision**), I am satisfied that such processing was likely to result in a high risk to the rights and freedoms of child users of Instagram.

In circumstances where Facebook Ireland Limited has not conducted an assessment of the impact of such processing operations on the protection of personal data (a “Data Protection Impact Assessment”) I find that Facebook Ireland Limited has not complied with its obligations under Article 35(1) GDPR.

Was a DPIA required in respect of the public-by-default processing?

398. I have next considered whether the public-by-default processing by FB-I required an assessment of the impact of such processing operations on the protection of personal data, pursuant to Article 35(1) GDPR. The nature and scope of this processing is as described in Part C.3 of this Decision.

399. With regard to this processing, FB-I submits that relevant risks for the purpose of Article 35 are not evident in circumstances where the processing takes place in the context of *“a safety-focused Instagram Service”*.

400. In its submission of 18 December 2020, FB-I characterised³²⁷ the context of the public-by-default processing as follows:

“People choose to join Instagram to share with a global community of diverse users, discover new content, and explore shared interests. This purpose of the Service is also made clear to Users prior to registration. Thus, defaulting personal accounts’ audience settings to “public” is consistent with what Users expect and are told when joining the Instagram community. Coupled with the robust privacy and security features that Facebook Ireland developed for Instagram - including specifically with Teens in mind - having the audience setting for new profiles set to public in this way facilitates Users’ ability to connect with others and to explore and discover new content that brought them to Instagram in the first place, while ensuring they can do so safely.”

³²⁷ FB-I’s submission of 18 December 2020, page 3

401. Subsequent to the DPC's Statement of Issues letter, FB-I provided the DPC with an updated LIA, which includes³²⁸ an assessment of risks arising from the controller's decision to make Instagram profiles public at the point of registration³²⁹. This assessment included tables outlining the severity and likelihood of risks arising from the Instagram service, (as set out above at paragraphs 264 and 265). It is evident³³⁰ from FB-I's analysis in the LIA that it is aware of risks arising from making profiles public by default, and that it characterises these risks as having severe possible impacts on child users. In particular, the risk of communication between child users and dangerous individuals is expressly described in this context as a possible risk which may result in a severe impact for child users.

402. In order to assess whether the public-by-default processing results in a high risk for the purpose of Article 35(1) GDPR, I have considered the criteria set out in the DPIA guidance. In this regard, I note that making social media posts of child users visible (by default) to anyone (including persons who have not registered with FB-I as Instagram users) meets two of the relevant risk criteria. In particular, this processing relates to the personal data of vulnerable data subjects (children), and is carried out on a large scale (to the extent that social media posts of child users can be viewed globally by millions of people by default, on and off Instagram). I further note that by making social media posts and content of child users public by default, FB-I implemented a setting which made the social media accounts of child users much more visible than private profiles, increasing the risk of dangerous or abusive communication.

403. Without prejudice to the wider adequacy or compliance of FB-I's safety, security and transparency measures with the requirements of the GDPR (as addressed elsewhere in this Decision) I am satisfied for the purpose of Article 35(1) that the high risk threshold for conducting a DPIA has been met.

404. In response to the above views, FB-I submits³³¹ that the risks identified in the LIA are merely *potential* risks, which apply equally to both public account and private accounts. As I have addressed elsewhere in Part G.2 of this Inquiry report, I do not accept FB-I's submission that the risks enumerated in the LIAs are not relevant risks for the purposes of the GDPR, including Article 35 GDPR. It is also the case that "severe" risks, where they exist, should be accounted for by means of a DPIA; even if a controller is of the view that a risk has been mitigated, the obligation to be accountable for that risk under the GDPR may still exist. I also note that the risk of communication between dangerous individuals

³²⁸ "Legitimate Interests Assessment ('LIA') Processing minors' data for the provision of the Facebook Products", 28 January 2021, section 4.2

³²⁹ Such an assessment is also evident at page 39 of FB-I's LIA of 23 October 2020, Appendix H to FB-I's submission of 27 October 2020

³³⁰ Similar tables of risks were also contained in the previous LIA of 23 October 2020, Appendix H to FB-I's submission of 27 October 2020

³³¹ FB-I's submission of 9 August 2021, paragraphs 77 and 78

was more pronounced in the case of public Instagram accounts, because content posted by children with public accounts would have been more visible, and subject to less control in terms of audience. I therefore do not accept FB-I's submission in this regard.

405. FB-I submits for the same reasons set out at paragraph 394 above that child users should not be considered vulnerable in the context of the public-by-default processing. In this regard, I note that child users may not be aware of the risks arising from having a public account. I also note that survey cited above at paragraph 310 suggests that a significant percentage of child users experience difficulty in switching their social media accounts from public to private. When viewed in context, I am satisfied that child users should be considered as "vulnerable" for the purpose of the DPIA guidelines in connection with the public-by-default processing, because it is reasonably foreseeable that child users may not understand the risks associated with having a public account, or may experience some difficulty in switching to a private account.

406. FB-I further submits in this regard that the audience setting does not constitute large-scale processing for the purpose of the DPIA guidelines. In particular, FB-I contends that public account users have control over how much content they post on the platform, and choose to make their content private at any time. However, I note in this context that where a user posts content as part of a public profile, it is accessible to an audience of global individuals (on and off the Instagram platform) and indexed for search purposes on the Instagram platform. I am therefore satisfied that this processing meets the description of *large scale* for the purpose of the DPIA guidelines, because the geographical extent of the processing activity is very extensive. Accordingly I do not accept FB-I submission in this regard.

407. Having considered FB-I's submissions of 9 August 2021, I remain of the view that the contact information processing meets two of the risk criteria, as set out in the DPIA guidelines.

Conclusion and Finding 6

408. In circumstances where the processing at issue meets the risk criteria set out in the DPIA Guidelines and to the extent that the controller itself has identified risks which could result in severe and significant impacts on child users (which are corroborated by additional sources as cited in Part G of this Decision), I am satisfied that the public-by-default processing by FB-I results in high risks to the rights and freedoms of child users, for the purposes of Article 35(1) GDPR.

Finding 6

Having taken into account the nature, scope, context and purposes of the public-by-default processing by Facebook Ireland Limited (**i.e. operating a social media network which, by default, allows the social media posts of child users to be seen by anyone,**

and as described further in parts C and G of this Decision) I am satisfied that such processing was likely to result in a high risk to the rights and freedoms of child users of Instagram.

In circumstances where Facebook Ireland Limited did not conduct an assessment of the impact of such processing operations on the protection of personal data (a “Data Protection Impact Assessment”), I find that Facebook Ireland Limited has not complied with its obligations under Article 35(1) GDPR.

This finding does not relate to the modified Instagram registration process for child users, which was notified to the DPC by Facebook Ireland Limited in 2021.

I. Assessment of FB-I’s Compliance with Articles 24, 25 and 5(1)(c) GDPR

I.1 Compliance with Articles 24, 25, and 5(1)(c) GDPR

409. The DPC Statement of Issues included, as matters for determination, an assessment of whether FB-I has complied with its obligations under Articles 5(1)(c), 24 and 25 GDPR which concerns the principles of data protection by design and by default.

410. Article 24 GDPR concerns the overarching responsibilities of controllers such as FB-I, and the principle of accountability under the GDPR, as follows:

“

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.”

411. Recital 74 to the GDPR clarifies what is meant by “measures” in the context of Article 24, by emphasising that measures implemented to comply with the GDPR should be demonstrably “effective”, as follows:

“The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In

particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.”

412. The Statement of Issues included consideration of whether FB-I failed to comply with Articles 25(1) and/or 25(2) in relation to the contact information processing and the public-by-default processing, and the data minimisation principle under Article 5(1)(c) GDPR.

413. The EDPB has published Guidelines on Data Protection by Design and by Default, which summarise Article 25 as follows³³²:

“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.”

414. Article 25(1) GDPR requires that, before a controller begins to process personal data, it must design and implement **measures** and **safeguards** to ensure compliance with the GDPR and the protection of individual’s rights, as follows:

“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.”

415. The obligation to implement measures and safeguards described in Article 25(1) is referred to as **Data Protection by Design**.

416. The requirement of *effectiveness* is a key element of Article 25(1), as set out in the EDPB guidelines³³³:

“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

³³² Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 2

³³³ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, subchapter 2.1.2.

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.”

417. Article 25(2) GDPR requires controllers to implement **measures** to ensure that by default, the principle of data minimisation is respected, as follows:

“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.”

418. The obligation to implement measures described in Article 25(2) is referred to as **Data Protection by Default**.

419. Article 25 does not prescribe the implementation of any specific technical and organisational measures, or safeguards; the appropriate measures and safeguards must be identified by the controller, having considered the specific processing at issue.

I.2 Submissions by FB-I regarding Article 25 and 5(1)(c) GDPR

420. FB-I describes its overarching design approach to Instagram for child users, as follows³³⁴:

“To provide an appropriate environment for the sharing of content...Facebook Ireland is committed to fostering a safe and supportive community for everyone on Instagram – including teens between the age of 13 and 17...While they are in the

³³⁴ FB-I's submission of 27 October 2020, paragraph 3

minority of its users, Facebook Ireland recognizes that Teens are an important part of the Instagram community and therefore has designed Instagram with their safety specifically in mind. As such, in line with Instagram's vision statements, Facebook Ireland offers a safety-oriented Instagram service, which both facilitates sharing and expression while also addressing issues such as bullying, improving equity and fairness, and helping users feel supported."

421.FB-I further states³³⁵ that as a result of the measures and safeguards it implements, (discussed in Part F of this Decision) that it has provided:

"...a safe Instagram product to the entire Instagram community (including Teens), so that everyone can share content in line with the purpose of the service."

422.With regard to the public-by-default audience setting, FB-I submits³³⁶

"...[r]egardless of whether a user chooses to keep an account public, he or she can still make granular privacy choices to block and manage interactions with others on Instagram, and always has the ability to report inappropriate or harmful behaviour and content. As described in the introduction above, Facebook Ireland provides a suite of in-app safety tools and privacy and security features, all consciously designed with Teen safety in mind and which are available to Teens irrespective of whether they have a private or a public personal account. Facebook Ireland has also created a dedicated Parents Centre and Parents Guide with information, tips, and resources for parents to help them better navigate Instagram with their Teen.

...In this way, Facebook Ireland fulfils its obligations to Teens under Articles 24 and 25 and in accordance with Recitals 38, 75, and 76 GDPR to the extent they are engaged with respect to this processing. These measures include the continuous consideration, re-design, and improvement of existing processes and safeguards to best protect Teen Users in the context of the Instagram Service.

423.With regard to the publication of contact information of child users, FB-I submitted as follows³³⁷:

"...In the case of businesses and creators, both the world economy and professional opportunities online have evolved at great speed. The reality of how people do "business" in a digital environment -- i.e., what constitutes a business, how businesses are created, operate, and interact with customers or followers -- is very different today (in particular when taking account of the effects of a global pandemic) than in 2019; and than even earlier in 2016 when Business Accounts were first created. This is why the original development and roll-out of Business Accounts was focused on their

³³⁵ FB-I's submission of 27 October 2020, paragraph 6

³³⁶ FB-I's submission of 27 October 2020, paragraphs 52 and 53

³³⁷ FB-I's submission of 18 December 2020, paragraphs 43 and 44

utilisation by more “traditional” businesses looking to bridge their off-Instagram presence to the platform, why the contact information functionality of Business Accounts at launch was appropriately tailored to use by such businesses, and why over time the use of Business Accounts evolved to a point where changes in this regard became appropriate.

...As a result, in recognition of the fact that the uses and needs served by these Business Accounts had evolved in this way, Facebook Ireland determined that the requirement for the public display of a contact option associated with a Business Account should be made optional. This change, for example, better accounted for the emergence of use of such accounts by other people or groups, like artists, bloggers, influencers, charitable organisations, social activists, or even small Instagram app-based businesses that may not have a “traditional” physical or off- Instagram presence (including other business contact information). Rather than any basis for criticism, this in fact illustrates that Facebook Ireland continually assesses whether original product designs that were appropriate at launch remain fit for their intended purpose over time, and makes appropriate changes where necessary.”

424.FB-I made a specific submission regarding whether the publication of contact information in the HTML of business account profile webpages was contrary to the principle of data minimisation under Article 5(1)(c) GDPR, as follows³³⁸:

“The Commission has inquired whether the presence of the email address in the HTML source code was in contravention of the GDPR’s data minimisation principles (e.g., Article 5(1)(c)). Facebook Ireland respectfully submits it is not. First, Facebook Ireland does not require the provision of any business contact email address – meaning any User whose email address appeared in the HTML source code in this way had chosen to convert to a Business Account (and specifically chosen a Business Account as opposed to a Creator Account) and to provide this business email address publicly. Second, as explained above, the inclusion of the contact email address in the HTML source code in these circumstances is what enabled the “email” button to render on Instagram Web in line with the relevant User’s choice. As a consequence of taking the email address out of the HTML source code, the “email” contact button functionality is no longer available for Business Accounts on Instagram Web. Finally, if a User chose to delete the contact point from his/her Business Account, it was no longer included in the HTML source code.”

I.3 Analysis and findings of the DPC

FB-I’s submission of 9 August 2021

³³⁸ FB-I’s submission of 18 December 2020, paragraph 57

425. In its submission of 9 August 2021, FB-I made a number of additional submissions³³⁹ to the DPC regarding the correct interpretation of Articles 24 and 25 GDPR. In particular, FB-I submits that Articles 24 and 25 GDPR are non-prescriptive and premised on the notion that controllers have flexibility in how they comply with these obligations. As with other aspects of this Inquiry, FB-I asserts that the DPC has incorrectly taken into account *potential risks*, which are not actual risks and which are not based on evidence, and which fail to take into account the potential benefits to child users which result from the processing at issue.
426. FB-I contends that it is not appropriate for the DPC to take “...a rigid or prescriptive approach to internal procedures or policies that organisations have in place”, on the basis that Article 24 is not prescriptive. FB-I supports the view that controllers must concrete measures to the specific nature of the processing being carried out. FB-I further cites the WP29 Opinion on Accountability³⁴⁰ (which relates to the Data Protection Directive) in support of the view that there is tension between the principle of accountability, and the objective of legal certainty.
427. With regard to Article 25 obligations, FB-I cites the EDPB Guidelines³⁴¹ on Data Protection by Design and by Default, in support of its view that the task of implementing measures and safeguards is not prescriptive, and should be determined by the controller, with an allowance of flexibility as to the appropriate measures and safeguards.
428. FB-I’s above submissions appear to be predicated on the idea that there exists a presumption (in the context of Articles 24 and 25 GDPR) that measures and safeguards selected by a controller are *prima facie* appropriate and effective. However, this view is incongruous when assessed in light of the principles and provisions of the GDPR. The GDPR emphasises the need for controllers to be accountable and responsible for processing, and to be able to demonstrate compliance with the GDPR. While it is true that these provisions do not prescribe particular actions on the part of controllers, there is limited support for the idea that the legislative objective of the GDPR is to create a wide margin of *flexibility* for actions by controllers. While measures and safeguards may not be prescribed, the quality and nature of these measures is described in detail, thereby defining the obligations of the controller in concrete terms.
429. With regard to the specific facts of this Decision, the DPC does not accept FB-I’s view that the controller is entitled to a greater margin of flexibility and discretion in the measures and safeguards it implements. The DPC for its part is obliged to assess whether the controller has implemented appropriate and effective measures and safeguards. In conducting this assessment, the DPC has not applied arbitrary criteria; rather, it has assessed the concrete measures and safeguards implemented by the controller. The DPC

³³⁹ FB-I’s submission of 9 August 2021, paragraphs 87 to 96

³⁴⁰ WP29, Opinion 3/2010 on the principle of accountability (July 2010)

³⁴¹ EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (October 2020)

has obtained FB-I's submissions on the adequacy and effectiveness of the measures and safeguards which were selected and implemented by FB-I, as well as submissions on the relevant factual considerations addressed in Part G of this Decision. Accordingly, I do not accept FB-I's submissions in this regard.

430. FB-I further submits³⁴² in this context that the DPC must accept that “[s]ome potential or theoretical risk is an unavoidable part of Teens learning to be independent – both with any online or offline venture or experience”. While FB-I's comparison of real-world risk and online risk is specious (on account of the granular level of control that FB-I can, as a matter of fact, exercise on its platform), I accept that the GDPR does not require the absolute elimination of risk, and instead considers questions of risk in context. FB-I suggests in particular that it was reasonable to publish the email addresses and phone numbers of child users, to avoid “*shutting Teens out entirely*” of the business account functionality. FB-I submits that the benefits of this form of publication outweighed the risks. Having considered this point, I am not convinced by FB-I's submission. Publishing phone and email contact information of child users (as young as 13 years old) is clearly linked to high risks, as described above in Part G. Balanced against this risk was the “benefit” of being contactable to unknown persons off Instagram. Off-Instagram contact information was a relatively minor aspect of the business account functionality (primarily relevant to bricks-and-mortar businesses, not children). This processing was clearly not essential to carrying out a professional activity on Instagram (a service which of itself provides direct modes of engagement and communication). Accordingly, I do not agree with FB-I conclusion that the benefits outweighed the risks with regard to this processing.

431. FB-I also contends that the public-by-default processing struck a “*reasonable balance between mitigating those risks while enabling the exercise of Teen Users' broader rights and freedoms*”. In this regard, it does not appear that a proper balance was struck by FB-I; there are high risks associated with making the accounts of child users public by default, and yet the claimed benefit which purportedly offsets the risks to child users (i.e. unfettered engagement with a social network) could equally be obtained by operating a private Instagram account.

432. With regard to the interpretation of Article 5(1)(c) GDPR, FB-I submits³⁴³ that this principle does not require the reduction of processing to the absolute minimum, on the basis that the Court of Justice of the European Union has held³⁴⁴ that the data minimisation principle gives “*expression to the principle of proportionality*”. FB-I also cites the EDPB Article 25 Guidelines³⁴⁵ regarding the interpretation of the “*amount*” of personal data in the context of Article 25(2), insofar that the guidelines state that the

³⁴² FB-I's submission of 9 August 2021, paragraphs 99 and 102

³⁴³ Ibid, paragraphs 107 and 108.

³⁴⁴ CJEU, judgment dated June 22, 2021, C-439/19, para. 98 – Latvijas Republikas Saeima

³⁴⁵ EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020

correct amount of personal data to be processed “will have to be assessed by controllers depending on the circumstances of their intended processing operations”.

433. With regard to the DPC’s assessment of Article 24 GDPR, FB-I also submits as follows³⁴⁶:

“...non-compliance with Article 35 GDPR cannot automatically equate to non-compliance with Article 24 GDPR. Article 24(1) GDPR, for example, is a broader, more generalised, non-prescriptive, and more holistic accountability obligation than being able to produce a DPIA on demand, and processing can be compliant with Article 24 GDPR even where there is no DPIA in place. In other words, even where a DPIA is not carried out, it cannot be said that a controller has not considered the “risks of varying likelihood and severity for the rights and freedoms of natural persons” posed by the processing for purposes of Article 24 GDPR compliance.”

FB-I contends that a controller should not automatically be found to have infringed Article 24 GDPR if it has conducted a “good faith” DPIA screening assessment.

434. I accept that Article 24 is drafted in such a manner that a broad range of measures may be relied upon by a controller to demonstrate compliance with the GDPR. At the same time, it is clear that the DPIA obligation under Article 35 GDPR (where it applies to processing) constitutes a mode of *demonstrating* compliance with the GDPR (insofar as it involves a record of the controller’s “*identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk*”³⁴⁷). On this basis, a failure to comply with the requirements of Article 35 GDPR can also be regarded as a failure to demonstrate compliance with the GDPR for the purpose of Article 24 GDPR. A “good faith” screening exercise which incorrectly discounts the need for a DPIA is not a substitute for the full assessment of risk required under Article 35 GDPR (where such an assessment is required). In the present circumstances, I am satisfied (for the reasons described in Parts G and H of this Decision) that the processing at issue resulted in high risks for child users for the purposes of Article 35 GDPR, and therefore the controller was subject to the requirement to produce a DPIA. Having failed to produce a DPIA (which is an express requirement of the GDPR, and not a flexible obligation), and having no alternative mode of demonstrating how it has identified and mitigated the high risks which exist, the controller cannot be regarded as being “*able to demonstrate that processing is performed in accordance with*” the GDPR. I therefore satisfied that a failure to comply with Article 35 GDPR may properly be construed as a failure to demonstrate compliance with the GDPR, for the purpose of Article 24 GDPR.

³⁴⁶ FB-I’s submission of 9 August 2021, paragraphs 84 to 86

³⁴⁷ Recital 77 GDPR

Assessment and conclusions regarding FB-I's compliance with Articles 24, 25 and 5(1)(c) in connection with publication of email and/or phone contact information of child users

435. Article 5(1)(c) GDPR requires that personal data should be “adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed”.

436. With regard to FB-I's compliance with Article 5(1)(c) GDPR, I note that FB-I made phone and/or email contact information of child users easily accessible to anyone on or off Instagram, by including this information as plain text in the HTML source code for certain Instagram profile webpages. FB-I states that this processing was intentional on its part, and a necessary consequence of the child users' decision to publish their contact information to the world at large when switching to a business account. Notwithstanding this position, FB-I has (on two separate occasions) removed the contact information from all webpage profiles when this practice was brought to the attention of the Facebook Security Team by Mr Stier. In particular, when abandoning the HTML publication of contact information in March 2019, a representative with the Facebook Security Team informed Mr Stier “After discussing this functionality with the Instagram team we did take steps to remove the contact information from the HTML of the page, since it was not necessary to include in its current form”. As such, FB-I's submission that this HTML processing was necessary is directly contradicted by the actions and words of the Facebook Security Team. FB-I states that this processing was necessary to provide business accounts to child users, who would otherwise be impeded in promoting their professional activities on Instagram; whereas the Facebook Security Team stated expressly that this processing was not necessary, and stopped this practice immediately when it was brought to its attention.

437. In this instance, the purposes of processing³⁴⁸ were adequately served by the optional inclusion of contact information in the Instagram application, without the need for the inclusion of a “contact button” on the web version of Instagram. It is also clear that many business account users did not require the publication of personal contact information in order to pursue their professional purposes on Instagram³⁴⁹. I am therefore satisfied that the mandatory publication (prior to 7 March 2019) of contact information on the website version of Instagram (in HTML) for all business account users had the result that the personal data at issue (i.e. contact information of child users on webpages) was not limited to what was necessary in relation to the purposes for which FB-I processed this specific information, contrary to the data minimisation principle under Article 5(1)(c) GDPR.

438. Prior to 7 March 2019, the phone numbers and/or email addresses of those child users of Instagram with business accounts were made accessible by default in the HTML source

³⁴⁸ As discussed in Part G.1 of this Decision

³⁴⁹ As per footnote 16 to FB-I's submission of 27 October 2020

code of business account profile webpages. This processing was conducted to a global extent, and resulted in dissemination of personal data to an indefinite number of natural persons, contrary to the principle of data protection by default as set out in Article 25(2) GDPR.

439. In its submission of 9 August 2021, FB-I reiterates³⁵⁰ its view that the contact information processing was consistent with the *purpose* of the business account function, and formed a “*core and essential feature*” at the time business accounts were first implemented.

440. FB-I’s overarching contention therefore (as set out in Paragraph 420 above) is that Instagram business accounts were designed for traditional businesses in 2016, and were subsequently modified in 2019 to account for novel types of online professional activity. I acknowledge that professional activities of Instagram users may have intensified and changed since 2016. However, it is difficult to accept FB-I’s contention that the professional features on its platform were created at a time before the prevalence of social media influencers; it is apparent from contemporaneous media coverage of Instagram³⁵¹ that the concept of a social media “influencer” was well established by 2016. The existence of these types of small-scale professional users would have been known to FB-I at the time it first implemented business accounts. FB-I nevertheless contends that the contact information feature was initially intended only for users who wished to link their “*off-Instagram*” presence to their Instagram account (i.e. business accounts were not intended for types of professionals who did not already have an off-Instagram professional presence, such as small-scale social media influencers).

441. FB-I contends that the modification of business accounts in July and September 2019 (over a year after the application of the GDPR) should not be a “*basis for criticism*” in circumstances where FB-I “*continually assesses whether original product designs that were appropriate at launch remain fit for their intended purpose over time, and makes appropriate changes where necessary*”. I disagree with this statement, for the reason that the requirement to publish contact information was clearly not “*appropriate*” as of May 2018. Traditional businesses (with separate off-Instagram presences in the real world or online) are not typically operated by children. Since the application of the GDPR in May 2018, FB-I has been aware of the age of child users who register on Instagram. FB-I therefore had clear information as of May 2018 concerning which of its users were likely not to be “traditional businesses”.

442. Notwithstanding this, FB-I facilitated all child users in switching to business accounts (prior to July 2019) without any effective limitations or safeguards. The default position

³⁵⁰ FB-I’s submission of 9 August 2021, paragraph 117

³⁵¹ ["Luka Sabbat, the 18-Year-Old Fashion Influencer"](#), The New York Times, 8 April 2016

["How to make money as a digital influencer"](#) The Financial Times, 1 November 2016

["How online 'influencers' are changing the food industry"](#), bbc.com, 13 May 2016

in May 2018 (before the introduction of opt-outs and creator accounts in 2019) was that child users, known by FB-I to be as young as 13, would have full unrestricted access to features intended for traditional businesses. This decision by FB-I resulted in the mandatory publication of the personal contact information of child users (without the ability to opt-out).

443. 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 (in particular with regard to the extent of the processing). In this case, prior to July 2019, FB-I's stated purpose for publishing contact information of business accounts was to provide traditional businesses with a "bridge" to their off-Instagram presences (such as the phone number for a restaurant, or the website of a bank). By FB-I's own account³⁵², the purpose of this processing did not initially encompass the on-platform professional activities of new types of professional Instagram users (until separate features were launched in July 2019 to account for such users). It follows that FB-I processed the contact information of child users for a purpose that was intended only for traditional businesses. Child users and traditional businesses were clearly two distinct categories of Instagram user. It was technically possible at relevant times for FB-I to identify child users, based on age information obtained during the Instagram registration process.

444. In its submission of 9 August 2021, FB-I objects³⁵³ to this conclusion on the basis that a cohort of child users might have had a legitimate business requirement to publish phone and email contact information prior to September 2019, in circumstances where FB-I could not distinguish such users from other child users who did not have such a purpose of processing. FB-I contends that it would conflict with its role as an intermediary platform provider to make individual decisions on the business requirements of specific child users. To be clear, the DPC has not proposed alternative measures or safeguards by which FB-I might have complied with the data minimisation principle; it is not the position of the DPC that FB-I ought to have assessed the *bona fides* of each user's business activities. The role of the DPC is to assess the processing implemented by FB-I, and the measures and safeguards implemented. Accordingly, FB-I's contention that it acts an "*intermediary platform provider*" is of limited relevance to the determination of this Inquiry; however FB-I defines its role, it must comply with the GDPR.

445. FB-I designed and implemented the Instagram business account function. The business account function was initially intended for "*traditional businesses*"³⁵⁴. The publication of contact information for traditional bricks-and-mortar businesses was a reasonably foreseeable business requirement. However, in direct contradiction to its stated

³⁵² FB-I's submission to the DPC of 27 October 2020, footnote 16, page 9

³⁵³ FB-I's submission of 9 August 2021, paragraph 118

³⁵⁴ FB-I's submission of 27 October 2020, paragraph 10

intention of providing business features to traditional businesses, FB-I also allowed child users (including children as young as 13) to access the full suite of business features, including a requirement that the child's phone and email contact details be made public. FB-I contends that it was reasonable to treat child users the same as banks and travel agents, because some child users may have had a professional requirement to publish their phone and email contact information. In my view, FB-I's contention that all child users had a potential business requirement to "bridge" their different professional identities (i.e. by publishing phone and email contact information) is not a reasonable conclusion on the *purpose of processing* in the context of Article 5(1)(c) GDPR. I am further of the view that, even if a limited cohort of child users had a professional requirement to publicly share phone and email contact details, the extent and amount of processing of personal data by FB-I with regard to the contact information of children was not necessary or proportionate. The need to create links between professional business identities is not a typical requirement of children as a class of persons - especially younger children.

446. Accordingly, the extent that prior to July 2019 FB-I processed the contact information of child users by default for a purpose that was intended only for traditional businesses, FB-I failed to ensure that only personal data which were necessary for the specific purpose of this processing were processed.

Finding 7

Prior to 7 March 2019, Facebook Ireland Limited published email addresses and/or phone numbers of child users of Instagram in the HTML source code of certain Instagram profile webpages. In circumstances where the personal data processed by Facebook Ireland Limited in this regard were not limited to what was necessary in relation to the purposes for which FB-I processed this specific information, I find that Facebook Ireland Limited did not comply with the principle of data minimisation as set out in **Article 5(1)(c) GDPR**.

I am further of the view that, prior to 7 March 2019, Facebook Ireland Limited failed to implement appropriate technical and organisational measures with regard to the HTML publication of contact information to ensure that, by default, only personal data which were necessary for this specific purpose of processing were processed. In particular, this processing was performed to a global extent, and in circumstances where Facebook Ireland Limited did not implement measures to ensure that by default the contact information of child users was not made accessible without the individual's intervention to an indefinite number of natural persons. I am therefore of the view that the above processing by Facebook Ireland Limited was contrary to the principle of data protection by default under **Article 25(2) GDPR**.

Prior to July 2019, as an element of the provision of business accounts on the Instagram social network, Facebook Ireland Limited required and implemented the publication of email addresses and/or phone numbers of child users of Instagram. This

processing resulted in the global dissemination of personal data of child users who had business accounts on Instagram, without the ability to opt-out of publication.

In this regard, I am of the view that Facebook Ireland Limited failed to implement appropriate technical and organisational measures to ensure that, by default, only personal data which were necessary for this specific purpose of processing were processed.

In particular, this processing was performed to a global extent, and in circumstances where Facebook Ireland Limited did not implement measures to ensure that by default the contact information of child users was not made accessible (without the user's intervention) to an indefinite number of natural persons. I am therefore of the view that the above processing by Facebook Ireland Limited was contrary to the principle of data protection by default under Article 25(2) GDPR.

447. In Part G of this Decision I have considered:

- the nature, scope, context and purposes of FB-I's processing in connection with the publication of contact information of child users of Instagram between 22 February 2019 and 21 September 2020;
- the risks posed to the rights and freedoms of child users of Instagram as a result of this processing; and
- whether the measures and safeguards adopted by FB-I were sufficient for the purposes of Articles 24 and 25 GDPR.

448. As is set out above, I am of the view that the processing at issue poses a severe risk that dangerous individuals may communicate directly with children. I agree with the assessment of risk in FB-I's LIA³⁵⁵ that such communication may result in "*grooming; physical, sexual and emotional abuse; [and/or] trafficking*", including communication risks arising "*from a user choosing to display contact details or the risk that the communication **could be taken off platform***" (emphasis added). I also note that email and phone contact information in HTML may be targeted for web-scraping, or otherwise obtained by unauthorised third-parties, giving rise to a significant possible risk of fraud and impersonation.

449. Although the GDPR principle of data protection by design did not apply at the time when business accounts were first implemented by FB-I in 2016, the obligation to implement appropriate measures and safeguards applied to this ongoing processing as of May 2018³⁵⁶. I also note in the context of Article 25(1) GDPR that this processing did not

³⁵⁵ Part 4.2.a of the LIA of 28 January 2021

³⁵⁶ Article 25(1) applies on a prior basis, but also applies "*at the time of the processing itself*"

comply with the principles of data minimisation and data protection by default, as set out in Findings 7, 8 and 9 above. Having considered (in Part G.3 of this Decision) the measures and safeguards implemented by FB-I in respect of the contact information processing, I am of the view that the measures and safeguards that were implemented by FB-I failed to implement the requirements of the GDPR or to protect the rights of child users, as required under Article 25(1) GDPR.

450. In this context, FB-I contends³⁵⁷ that the principle of privacy by default has not been infringed, on the basis of the account switching process was designed in such a way that *“any Users that continue to switch to a Business Account, and display contact information as part of that, do so at their own election, in a fully informed manner, and in order to avail themselves of that functionality”*. In this regard, I am not satisfied that the switching process had adequate design elements to prevent inadvertent or inappropriate publication of contact information of child users, and I refer to the detailed treatment of this issue as set out in Part G.2 of this Decision.

Finding 8

Prior to 4 September 2019, Facebook Ireland Limited required and implemented the publication of email addresses and/or phone numbers of child users of Instagram in the context of Instagram business accounts, without the ability to opt-out of publication.

This processing included publication of email and/or phone contact information in the HTML source code of profile webpages of child users who switched to an Instagram business account.

At the time of commencement of this Inquiry, Facebook Ireland Limited continued to facilitate and implement the publication of email addresses and/or phone numbers of child users of Instagram in the context of Instagram business accounts.

The above processing poses severe possible risks to the rights and freedoms of child users.

In circumstances (described in Part G of this Decision) where Facebook Ireland Limited did not implement appropriate technical and organisational measures which were or are designed:

- to implement data-protection principles in an effective manner; and
- to integrate the necessary safeguards,

into the above processing in order to meet the requirements of the GDPR and to protect the rights of child users of Instagram, I find that Facebook Ireland Limited has not complied with its obligations under Article 25(1) GDPR.

³⁵⁷ FB-I's submission of 9 August 2021, paragraph 119

451. Article 24 GDPR establishes the responsibility and liability of controllers for processing of personal data. In particular, Article 24 requires that controllers adopt risk-based measures:

- to ensure compliance with the GDPR; and
- to demonstrate compliance with the GDPR.

Where proportionate, the measures required under Article 24 may include the implementation of appropriate data protection policies by the controller.

452. Recital 75 GDPR outlines the types of risks that must be taken into account by controllers when implementing accountability measures for the purposes of Article 24, including risks where personal data of children are processed, or where processing involves a large amount of personal data and affects a large number of data subjects.

453. For the purposes of assessing FB-I's compliance with Article 24 GDPR in relation to the processing of contact information of child users, I have considered, in Part G of this Decision, the nature, scope, context and purpose of this processing. Having considered these four factors, I have concluded, in Part G.2 of this Decision, that the processing of contact information of child users results in a severe possible risk to the rights and freedoms of child users, to the extent that dangerous individuals may use this contact information to communicate with child users, and to the extent that contact information may be collected by unauthorised persons for the purposes of fraud and/or impersonation.

454. FB-I has outlined the risk-based measures it has implemented for the purpose of ensuring and demonstrating its compliance with the GDPR with regard to this processing. I have considered these measures in Part G.3 of this Decision. While I accept that FB-I provides certain information and tools to users, which promote safety and prevent bullying on the Instagram platform, I am of the view that these limited measures are not effective in circumstances where severe possible risks are posed by off-Instagram publication of contact information of child users, and potential off-Instagram communication which could result from publication of contact information. I am therefore of the view that FB-I has not properly taken into account the risks posed to the rights and freedoms of child users when implementing measures to ensure its compliance with the GDPR. I also note in this regard that FB-I has not conducted a DPIA in respect of this high-risk processing, as described in Part G of this Decision. As a consequence of the failure to carry out a DPIA as required under the GDPR, FB-I is not able to demonstrate to the extent required under the GDPR how it complies with the GDPR in respect of this processing.

<u>Finding 9</u>

Prior to 4 September 2019, Facebook Ireland Limited required and implemented the publication of email addresses and/or phone numbers of child users of Instagram in the context of Instagram business accounts, without the ability to opt-out of publication.

This processing included publication of email and/or phone contact information in the HTML source code of profile webpages of child users who switched to an Instagram business account.

At the time of commencement of this Inquiry, Facebook Ireland Limited continued to facilitate and implement the publication of email addresses and/or phone numbers of child users of Instagram in the context of Instagram business accounts.

The above processing posed severe possible risks to the rights and freedoms of child users, as set out in Part G.2 of this Decision.

In circumstances (described in Part G.3 of this Decision) where Facebook Ireland Limited has not properly taken into account the risks posed by the above processing, I am of the view that Facebook Ireland Limited has not implemented appropriate technical and organisational measures **to ensure** that the above processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR.

In circumstances where Facebook Ireland Limited did not conduct a DPIA in respect of the above processing, I am also of the view that Facebook Ireland Limited has not implemented appropriate technical and organisational measures **to demonstrate** that the above processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR.

Assessment and conclusions regarding FB-I's compliance with Articles 24, 25 and 5(1)c) in connection with the public-by-default Instagram processing

455. For the purposes of this Decision, I have considered whether processing in connection with the public-by-default Instagram audience setting was in compliance with FB-I's obligations under Article 5(1)(c) GDPR (the data minimisation principle), and Article 25(2) GDPR (the principle of data protection by default).

456. I do not accept FB-I's contention that the sole or primary purpose of Instagram is the open sharing of social media content with anyone on or off Instagram. While open sharing of content is one valid purpose of the service, many Instagram users choose to share content with approved followers only, and restrict who can see their content by switching their accounts to "private". It is clear that there are two distinct user expectations as to the visibility of social media content, which are reflected by the public/private audience setting.

457. Of the [REDACTED] child users of Instagram in the European Region, a sizeable cohort registered with the expectation that they would share content only with people they approved, and not with the world-at-large. I accept that many Instagram users wish to avail of more extensive publication of their social media posts, and that it was possible, after registration, to change account settings to “private”. Notwithstanding this, FB-I implemented a public-by-default audience setting for all child users, without distinction or the prior ability to make an account private. The registration process at the time of commencement of this Inquiry made no reference whatsoever to public or private audience settings, or the possibility that the user could make their content private. In circumstances where child users may not be aware of the risks, consequences and safeguards in relation to processing, the public-by-default audience setting created conditions where the personal data of child users could be published to an indeterminate global audience before the child user had noticed the default setting implemented by FB-I, or had identified the Instagram settings for restricting access to their account. This practice by FB-I had the result that the personal data of child users who wished to avail of a private Instagram account was not limited to what was necessary in relation to this purpose of processing.

458. In its submission of 9 August 2021, FB-I contends³⁵⁸ that the public-by-default processing does not constitute a discrete purpose of processing. I do not accept this submission, for reasons that are set out in detail in Paragraph 74 above. FB-I reiterates its view that the public-by-default processing was relevant and necessary to further “Instagram’s core purpose”, and also submits that the DPC has otherwise, in the context of Part E of this Decision, accepted the necessity of core aspects of the Instagram service, including the public-by-default processing. I do not accept this submission for reasons that are set out in detail in Paragraph 81 above. FB-I also submits that it has acted within the “flexibility” afforded to it in deciding the correct amount of personal data to be processed as part of its service. While I accept that the data minimisation principle is an expression of the principle of proportionality, the controller’s discretion or flexibility in how it complies with this principle is not open ended. FB-I also submits that the user is able to control the extent of processing, the amount of personal data processed, and the audience for content. While this summary of privacy controls is generally accurate, I am nevertheless of the view that the default processing arrangement implemented by FB-I for child users was not necessary or proportionate, on the basis that child users may have had a reduced ability to apply privacy settings which were switched to public by default, on the basis that processing in the context of public accounts was global in extent, and on the basis that the processing was not necessary for the cohort of child users who did not wish to operate a public Instagram account.

³⁵⁸ FB-I’s submission of 9 August 2021, paragraphs 109 to 115

Finding 10

At the time of commencement of this Inquiry, Facebook Ireland Limited implemented a default Instagram account setting for child users which allowed anyone (on or off Instagram) to view social media content posted by child users on Instagram.

In this regard, I am of the view that Facebook Ireland Limited failed to implement appropriate technical and organisational measures to ensure that, by default, only personal data which were necessary for this specific purpose of processing were processed.

In particular, this processing was performed to a global extent, and in circumstances where Facebook Ireland Limited did not implement measures to ensure that by default the social media content of child users was not made accessible (without the user's intervention) to an indefinite number of natural persons. I am therefore of the view that the above processing by Facebook Ireland Limited was contrary to the principle of data protection by default under Article 25(2) GDPR, and contrary to the data minimisation principle under Article 5(1)(c) GDPR.

459. In Part G of this Decision I have considered:

- the nature, scope, context and purposes of FB-I's processing of personal data of child users resulting from the public-by-default audience setting;
- the risks posed to the rights and freedoms of child users of Instagram as a result of this processing; and
- whether the measures and safeguards adopted by FB-I were sufficient for the purposes of Articles 24 and 25 GDPR.

460. As is set out above, I am of the view that the processing at issue makes the social media content of child users visible to anyone on or off the Instagram platform. This increased visibility of child users on Instagram poses a severe possible risk that dangerous individuals may communicate directly with child users. I agree with FB-I's assessment³⁵⁹ that such communication may result in "*grooming; physical, sexual and emotional abuse; [and/or] trafficking*", including communication the risk that "*communication **could be taken off platform***" (emphasis added).

461. In its submission to the DPC, cited above at paragraph 422, FB-I cites the on-platform controls and tools it implemented on Instagram, and the information resources it has

³⁵⁹ Part 4.2.a of the LIA of 28 January 2021

provided to child users and their parents, as complying with the principle of data protection by design³⁶⁰ under Article 25(1) GDPR.

462. Having considered (in Part G.3 of this Decision) the measures and safeguards implemented by FB-I in respect of the contact information processing, I am of the view that these measures and safeguards do not properly take into account the specific risks to the rights and freedoms of child users which are at issue. In particular, as of the time of commencement of this Inquiry, FB-I allowed adult Instagram users to send private direct messages to child users. These messages could include photographic or video content. Although FB-I applies certain machine-learning safeguards and reporting mechanisms in the context of Instagram, the content of direct messages between child users and other users appears to be private. In this way, dangerous individuals could identify child users of Instagram by their public social media content, and could send abusive messages to child users by direct message. While the child user could report an abusive message retroactively, this would not prevent damage and harm to child users who had already been exposed to such material. The Instagram direct message function could also be used to persuade a child user to communicate off-Instagram, or to meet in person. I also note in the context of Article 25(1) GDPR that this processing does not comply with the principles of data minimisation and data protection by default, as set out in Finding 10 above. Having considered the risks posed, I am of the view that the measures and safeguards that were implemented by FB-I failed to implement the requirements of the GDPR or to protect the rights of child users, as required under Article 25(1) GDPR.

Finding 11

At the time of commencement of this Inquiry, Facebook Ireland Limited implemented a default Instagram account setting for child users which allowed anyone (on or off Instagram) to view social media content posted by child users on Instagram.

The above processing posed severe possible risks to the rights and freedoms of child users.

In circumstances (described in Part G of this Decision) where Facebook Ireland Limited did not implement appropriate technical and organisational measures which were or are designed:

- to implement data-protection principles in an effective manner; and
- to integrate the necessary safeguards,

³⁶⁰ Although the public-by-default audience setting may pre-date the application of the GDPR, the principle of data protection by design applied to this processing as of May 2018

into the above processing in order to meet the requirements of the GDPR, and in order to protect the rights of child users of Instagram, I find that Facebook Ireland Limited has not complied with its obligations under Article 25(1) GDPR.

463. For the purposes of assessing FB-I's compliance with Article 24 GDPR in relation to the public-by-default audience setting, I have considered, in Part G.1 of this Decision, the nature, scope, context and purpose of the processing which results from this setting. Having considered these four factors, I have concluded, in Part G.2 of this Decision, that the processing of contact information of child users results in a severe possible risk to the rights and freedoms of child users, to the extent that dangerous individuals may use this contact information to communicate with child users.

464. FB-I has outlined the risk-based measures it has implemented for the purpose of ensuring and demonstrating its compliance with the GDPR with regard to this processing. I have considered these measures in Part G.3 of this Decision. While I accept that FB-I provides certain information, tools and safeguards to users, which promote safety and prevent bullying on the Instagram platform, I am of the view that these limited measures were not effective in circumstances where child users could receive abusive direct messages on Instagram from dangerous individuals. I am therefore of the view that FB-I has not properly taken into account the risks posed to the rights and freedoms of child users when implementing measures to ensure its compliance with the GDPR. I also note in this regard that FB-I has not conducted a DPIA in respect of this high-risk processing, as described in Part H of this Decision. As a consequence of the failure to carry out a DPIA as required under the GDPR, FB-I is not able to demonstrate to the extent required under the GDPR how it complies with the GDPR in respect of this processing. I further note that by implementing a public-by-default audience setting, and therefore expecting all child users as young as 13 years old to have sufficient technical knowledge to change this setting, FB-I has created conditions in which unnecessary publication of child users' social media content may occur (i.e. more extensive processing of social media content than was intended by the user).

Finding 12

At the time of commencement of this Inquiry, Facebook Ireland Limited implemented a default Instagram account setting for child users which allowed anyone (on or off Instagram) to view social media content posted by child users on Instagram.

The above processing posed severe possible risks to the rights and freedoms of child users, as set out in Part G.2 of this Decision.

In circumstances (described in Part G.3 of this Decision) where Facebook Ireland Limited did not properly take into account the risks posed by the above processing, I

am of the view that Facebook Ireland Limited did not implement appropriate technical and organisational measures **to ensure** that the above processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR.

In circumstances where Facebook Ireland Limited did not conduct a DPIA in respect of the above processing, I am also of the view that Facebook Ireland Limited has not implemented appropriate technical and organisational measures **to demonstrate** that the above processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR.

J. Decision on Corrective Powers

465. I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my findings that FB-I has infringed the following articles of the GDPR in respect of its public-by-default processing: Articles 12(1), 35(1), 5(1)(c), 25(2), 25(1) and 24(1).

466. I have also set out above my findings that FB-I has infringed the following articles of the GDPR in respect of its contact information processing: Articles 6(1), 12(1), 5(1)(a), 35(1), 5(1)(c), 25(2), 25(1) and 24(1).

467. 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) and, if so, which corrective powers.

468. 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...”

469. 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) of the 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 require FB-I to bring its processing into compliance with the GDPR in the manner specified below;
- (2) A reprimand pursuant to Article 58(2)(b) of the GDPR; and

- (3) Ten proposed administrative fines in the ranges proposed at paragraph 626 below.

470. I set out further detail below in respect of each of these corrective powers that I propose to exercise and the reasons why I have decided to exercise them.

K. Order to Bring Processing into Compliance

471. Article 58(2)(d) of the 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”

472. In circumstances where I have found that the processing at issue was not in compliance with the GDPR, I have decided to make an order pursuant to Article 58(2)(d) GDPR. In particular, I have decided to order FB-I to bring the relevant processing into compliance with Articles 5(1)(a), 12(1), 35(1), 24(1), 5(1)(c), 25(2) and 25(1) GDPR. Further to the finding of infringement of Article 6(1) GDPR that was established by the EDPB, I have amended, as required by the Article 65 Decision³⁶¹, the terms of the order that were originally proposed by the Draft Decision to include an additional requirement for FB-I to bring the relevant processing into compliance with Article 6(1) GDPR.³⁶²

473. The order under Article 58(2)(d) applies to the extent (if any) that FB-I is conducting ongoing processing operations as described in Part C.3 of this Decision.

474. Specifically, to the extent that FB-I is engaged in ongoing processing as described in Part C.3, this order requires FB-I:

- (1) to provide child users with information in a clear and transparent form on the purposes of the public-by-default processing. This order is made further to Finding 1 and to ensure compliance with Article 12(1) of the GDPR.
- (2) to directly notify, using dynamic in-product notifications, all users of business accounts who switched to an Instagram business account between 25 May 2018 and 4 September 2019 and were children at that time, that FB-I has removed its requirement that child users publish their contact information on Instagram business profiles. This order is made further to Finding 4 and to ensure compliance with Article 5(1)(a) of the GDPR.
- (3) to conduct an assessment of the impact on the protection of personal data in respect of any ongoing contact information processing. This order is made further to Finding 5 and to ensure compliance with Article 35(1) of the GDPR in

³⁶¹ The Article 65 Decision, paragraph 134

³⁶² The Article 65 Decision, paragraph 242.

circumstances where I have found that this processing by FB-I (both before September 2019, and after) results in high risks to the rights and freedoms of child users.

- (4) to conduct an assessment of the impact on the protection of personal data in respect of any ongoing processing in connection with the public-by-default audience setting. This order is made further to Finding 6 and to ensure compliance with Article 35(1) of the GDPR in circumstances where I have found that this processing by FB-I results in high risks to the rights and freedoms of child users.
- (5) to implement appropriate technical and organisational measures in respect of any ongoing contact information processing. Such measures are to be designed to implement data-protection principles 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 child users of Instagram. This order is made further to Finding 8 and to ensure compliance with Article 25(1) of the GDPR. The technical and organisational measures should be guided by the DPIA ordered at point 3 of this order.
- (6) to implement appropriate technical and organisational measures in respect of any ongoing contact information processing. Such measures are to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. This order is made further to Finding 9 and to ensure compliance with Article 24(1) of the GDPR. The technical and organisational measures should be guided by the DPIA ordered at point 3 of this order.
- (7) to implement appropriate technical and organisational measures in respect of any ongoing public-by-default processing, for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This order is made further to Finding 10 and to ensure compliance with Articles 5(1)(c) and 25(2) of the GDPR.
- (8) to implement appropriate technical and organisational measures in respect of any ongoing public-by-default processing. Such measures are to be designed to implement data-protection principles 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 child users of Instagram. This order is made further to Finding 11 and to ensure compliance with Article 25(1) of the GDPR. The technical and organisational measures should be guided by the DPIA ordered at point 4 of this order.
- (9) to implement appropriate technical and organisational measures in respect of any ongoing public-by-default processing. Such measures are to ensure and to be able

to demonstrate that processing is performed in accordance with the GDPR. This order is made further to Finding 12 and to ensure compliance with Article 24(1) of the GDPR. The technical and organisational measures should be guided by the DPIA ordered at point 4 of this order.

- (10) to reassess, for the purpose of the contact information processing, its reliance on Articles 6(1)(b) and 6(1)(f) by reference to the assessments, deliberations and conclusions of the EDPB, as set out in paragraphs 80 to 100 (inclusive) and paragraphs 101 to 133 (inclusive) of the Article 65 Decision and to take the remedial action necessary to address the deficiencies identified by the EDPB in the said paragraphs and, if FB-I is unable to resolve the identified deficiencies, FB-I must cease the contact information processing unless and until it is in a position to identify an alternative legal basis for processing pursuant to Article 6(1) GDPR.

475. My decision to impose the above order is made to ensure that full effect is given to FB-I's obligations under Articles 5(1)(a), 6(1), 35(1), 25(1), 24(1), 5(1)(c) and 25(2). I consider that this order is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR. In order to ensure fairness and transparency in accordance with Article 5(1)(a), it is crucial that those child users of Instagram who decided to switch to Instagram business accounts between 25 May 2018 - 4 September 2019 are notified of the removal of FB-I's requirement that child users publish contact information. A direct notification by means of a dynamic in-product notice is essential to ensure that those users are aware of the nature of the change and to ensure that they can make a decision on how to exercise control over their personal data accordingly.

476. In circumstances where I have found that there is a high risk associated with FB-I's ongoing public disclosure of email addresses and/or phone numbers of child users of Instagram, even though that disclosure is no longer mandatory for business accounts, it is essential that FB-I conducts a DPIA in respect of this processing and that it implements appropriate measures pursuant to Articles 24(1) and 25(1) of the GDPR. In circumstances where I have found that there is a high risk associated with FB-I's ongoing public processing of children's Instagram accounts it is essential that FB-I conducts a DPIA in respect of this processing.

477. FB-I has notified the DPC that as of March 2021, child users of Instagram are provided with a public/private audience setting option as part of the registration process. However, many Instagram users will have registered before the introduction of this option. Without prejudice to the question of whether these recent changes might be said to achieve compliance with FB-I's obligations under the GDPR, I am satisfied that it is appropriate to make the above order in the interest of clarifying and remediating the infringements set out in this Decision. Therefore, it is essential for ongoing compliance that FB-I implements appropriate measures pursuant to Articles 12(1), 24(1), 25(1), 35(1), 5(1)(c) and 25(2) of the GDPR in respect of the relevant processing.

478. Regarding the public-by-default processing, FB-I made significant changes in March 2021. This includes the introduction of a registration process that allows the user to choose between a public or private account. This Decision does not make findings regarding the transparency of, or the appropriateness of the measures implemented in respect of FB-I's ongoing processing of personal data that enables child users to create public accounts on a non-default basis following the changes implemented by FB-I in March 2021. While this Decision does not consider the changes made in March 2021, nonetheless, FB-I is accountable for ensuring that its ongoing processing that allows the social media posts of children to be seen by anyone is compliant with the GDPR. In this regard, the DPC reserves its right to commence further statutory inquiries in respect of recent changes if necessary.

Additional service modifications by FB-I since the PDD

479. In its submission of 9 August 2021³⁶³, FB-I submits that certain additional information is now provided to users regarding the audience setting, including during the registration process, in the Instagram Help Center, and in an updated Parents guide. FB-I also submits in this context that it intends to make amendments to its Data Policy in future, and intends to notify users who switched to a business account prior to September 2019 of the removal of the requirement for publication of contact information. FB-I submits that these aspects of the corrective order are therefore not necessary. In circumstances where FB-I's voluntary modifications in this regard are described as intended future actions on the part of the controller which have not been effected, I am satisfied that this aspect of the corrective order remains necessary. This view is without prejudice to of the question of whether those voluntary steps referred to by FB-I achieve compliance with FB-I's obligations pursuant to the GDPR.

480. In relation to those aspects of the corrective order that require a DPIA in relation to the processing at issue, FB-I submits³⁶⁴ that it now has "an active DPIA" in respect of the processing, which was prepared by repurposing elements of its LIA (as provided to the DPC in the course of the Inquiry). FB-I has not provided the DPC with a copy of this active DPIA, and I have otherwise found in this Decision that the LIA did not meet the requirements of Article 35 GDPR. Without prejudice to the question of whether the DPIA prepared by FB-I in response to this Inquiry achieves compliance with FB-I's obligations under the GDPR, I am satisfied that it is appropriate to make the above order in the interest of properly clarifying and remediating the infringements set out in this Decision.

481. In its submission of 9 August 2021, FB-I also submits³⁶⁵ that child users who convert to a business account will in future no longer be asked to provide contact information for inclusion in their public profile, but may provide this information subsequently. In

³⁶³ FB-I's submission of 9 August 2021, paragraph 124

³⁶⁴ Ibid

³⁶⁵ Ibid

circumstances where this individual measure has yet to be implemented, and without prejudice to the question of whether this measure achieves compliance with FB-I's obligations under the GDPR, I am satisfied that it remains appropriate to make the above order in the interest of properly clarifying and remediating the infringements set out in this Decision.

482. FB-I also submits³⁶⁶ that the corrective order is not required on the basis that in the time since the PDD, it has again modified the account registration process, and now allows child users to choose their audience setting at the time of registration, with the default setting being "private". With regard to existing child users with public accounts, FB-I says that it intends to show existing users a notification regarding their audience setting. In circumstances where FB-I's voluntary measures have yet to be fully implemented, and without prejudice to the question of whether such measures achieve compliance with FB-I's obligations under the GDPR, I am satisfied that it remains appropriate to make the above order in the interest of properly clarifying and remediating the infringements set out in this Decision.

Period for compliance

483. It was proposed in the PDD that this order should be complied with within three months of the date of notification of any final decision. FB-I submits³⁶⁷ (in the event that the voluntary actions it proposes are not accepted) that it would need "at least six months to assess and implement" any "further changes" required by the DPC. FB-I does not explain how it calculated this period of time, although it does refer generally to the technical and organisational difficulties posed when modifying the Instagram service.

484. FB-I is a large multinational organisation with significant financial, technological and human resources at its disposal. Moreover, the interim period, prior to any such rectification to the current lack of information being provided to data subjects, will involve a serious ongoing deprivation of their rights. Moreover, the DPC has provided specific analysis to FB-I in relation to the correct interpretation of the transparency provisions in question, and the relevant factual considerations for the purposes of Articles 24, 25 and 35 GDPR. This specificity should negate any need for extensive engagement with the DPC during the period of implementation, and provides clarity for FB-I as to what objectives its very significant resources should be directed towards in order to comply with this order. As such, I am not satisfied that it would be impossible or indeed disproportionate to make an order in these terms, having regard to the importance of the data subject rights involved, the specificity of the order and FB-I's resources.

³⁶⁶ Ibid

³⁶⁷ Ibid. paragraph 126

Conclusion on Order to Bring Processing into Compliance

485. I consider that this order is necessary to ensure that full effect is given to FB-I's obligations in relation to the infringements 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 exercised. FB-I disagrees and states that a reprimand would suffice in the circumstances, on the basis that it is already voluntarily attempting to alter the documents to express the views set out in the PDD.

486. However, having regard to the non-compliance identified 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. The fact that FB-I has started to take steps to bring its information into compliance reduces the practical impact of the order on the controller's resources. On that basis, I am satisfied that the order is a necessary and proportionate action.

487. I therefore require FB-I to comply with the above order within three months of the date of notification of this Decision. Further to this, I require FB-I to submit a report to the DPC within that period detailing the actions it has taken to comply with the order.

L. Reprimand

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

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

489. I have decided to impose a reprimand on FB-I 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 a significant number of child users of Instagram and are serious in nature. 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. The reprimand is necessary and proportionate in addition to the order proposed in Part K of this Decision. While the order would require specific remedial action on the part of FB-I, 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 FB-I and other controllers or processors carrying out similar processing operations, in particular in respect of the processing of children's data. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that FB-I and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their

obligations on transparency, fairness, DPIAs, data minimisation, accountability, and data protection by design and by default.

M. Administrative Fines

490. Article 58(2)(i) of the 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”

491. This makes clear that the DPC may impose administrative fines in addition to, or instead of, the order and reprimand also proposed 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).

492. Article 83(1) of the 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.”

493. Article 83(2) of the 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.”

494. 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.

495. 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 every infringement 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 infringements. 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. I also note in this context that although I have considered the application of Article 83(2) factors to the Article 24 infringement, I am conscious that Article 83 does not specify an administrative fine in respect of infringements of Article 24 GDPR. Accordingly, I have considered Article 24 separately to other infringements, and I do not consider this infringement to be an aggravating factor with regard to the other infringements at issue, or an issue which is pertinent to my calculation of the administrative fines.

Assessment of the Article 83(2) Criteria

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

496. As noted in Part E of this Decision, the Board determined the existence of an additional finding of infringement of Article 6(1) GDPR in the context of the contact information processing. The Article 65 Decision includes, amongst other things, a requirement to impose an administrative fine in response to the Board's finding of infringement of Article 6(1) GDPR. This requirement has been included, firstly, at paragraph 239 of the Article 65 Decision, as follows:

"The EDPB however agrees with the reasoning of the NO SA in its objection. ... the EDPB considers that an administrative fine should be imposed for this infringement."

497. At paragraph 240, the Article 65 Decision reiterates:

"Therefore, the EDPB instructs the IE SA to consider the identified infringement of Article 6(1) GDPR in its determination on the administrative fines, by imposing a fine for the additional infringement, which is effective, proportionate and dissuasive in accordance with Article 83(1) and (2) GDPR."

498. It is clear, from the passages quoted above, that the Board agreed with the reasoning provided by the Norwegian SA in its objection dated 30 December 2021 (the "**Objection**"). In the circumstances, I have also had regard, in the assessments concerning the infringement of Article 6(1) GDPR set out below, to the views expressed by the Norwegian SA, as set out on pages 8 and 9 of the Objection.

499. On the basis of the Board's instruction, I have amended my original Article 83(2) assessment, set out immediately below, to incorporate reference to, and assessment of, the additional finding of infringement of Article 6(1) GDPR that was established by the Article 65 Decision.

500. As regards FB-I's right to be heard in relation to the assessment of the Article 6(1) infringement, FB-I was provided with copies of all of the objections that formed the basis of the Board's Article 65 Decision and was invited to furnish submissions in relation to all aspects of same. FB-I was provided with a further opportunity to be heard, following the adoption of the Board's decision, as regards any matters which required a final determination to be made by the DPC or, otherwise, in relation to which the DPC was required to exercise its own discretion. The assessments and determinations set out below take account of any and all submissions that were made by FB-I, including its final submissions that were furnished to the DPC under cover of letter dated 30 August 2022 ("the **Final Submissions**").

M.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;

501. In considering the nature, gravity and duration of FB-I's infringements, I have had regard to the analysis in Part G.1 of this Decision concerning the nature, scope and purposes of the public-by-default processing and the contact information 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.

502. FB-I initially indicated to the DPC that there are "[REDACTED] child users of Instagram in the European Region". In a cover letter to its submission of 9 August 2021, FB-I indicated that it had mistakenly provided incorrect information on the number of child users. FB-I provided updated user numbers to indicate that "Instagram has [REDACTED] monthly average Teen Users in the European Region", of which, [REDACTED] child users operate business accounts, and [REDACTED] child users operate creator accounts. The number of data subjects affected by FB-I's infringements of Articles 12(1), 35(1), 5(1)(c), 25(2), 24(1), and 25(1) GDPR regarding the public-by-default processing is therefore at least [REDACTED] users (i.e. all those child users that do not operate public creator/business accounts, which are public accounts). FB-I's infringement of Article 12(1) affected each of those data subjects because FB-I failed to provide information in a clear and transparent form to each of them regarding the purposes of the processing. Similarly, FB-I's infringement of Article 35(1) also affected each of those data subjects. Where the GDPR mandates DPIAs, it does so in order to ensure that the controller assesses the risks to the rights and freedoms of data subjects and identifies measures to address those risks. FB-I's infringement of Article 35(1) denied all child users of Instagram in the European Region a legislatively mandated assessment designed to protect their rights and freedoms. FB-I's infringements of Articles 24(1) and 25(1) affected each of those data subjects because the appropriate technical and organisational measures that FB-I failed to implement ought to have been in place in order to protect the rights and freedoms of each of those data subjects. Finally, FB-I's infringements of Article 5(1)(c) and 25(2) affected each of the data subjects because all of their accounts were set to public without first giving those data subjects a choice between public and private accounts. Therefore, all of child users of Instagram were denied the choice when registering, even if some of them would have opted for a public account anyway.

503. The number of data subjects affected by FB-I's infringements of Articles 12(1), 5(1)(a), 35(1), 5(1)(c), 25(2), 24(1), and 25(1) regarding the contact information processing is

likely to be significant, in light of the fact that there are currently [REDACTED] child users with business accounts. While it is possible that fewer child users operated business accounts at the relevant times, I also note that many child users would probably have been diverted to the alternative “creator account” after July 2019. On this basis, I am satisfied that the processing was likely to have affected hundreds of thousands of children. It is therefore obvious that there was a very significant number of child users that switched to professional accounts, and in particular, hundreds of thousands of children switched to a type of account that was intended for traditional businesses.

504. Where such child users switched to a business account prior to 4 September 2019, they were affected by the infringement of Article 12(1), because those children were denied information using clear and plain language on the purposes of that processing and the categories of recipients of their personal data. FB-I’s infringement of Article 5(1)(a) also affected each of those children who switched to a business account prior to 4 September 2019 because each of them ought to have been directly notified of FB-I’s removal of its requirement that child users publish contact information. FB-I’s infringement of Article 35(1) affected every child user of Instagram business accounts because a DPIA ought to have been conducted in respect of the risk to their rights and freedoms. FB-I’s infringements of Articles 24(1) and 25(1) also affected each of those children because the appropriate technical and organisational measures that FB-I failed to implement ought to have been in place in order to protect each of their rights and freedoms. Finally, FB-I’s infringements of Article 5(1)(c) and 25(2) also affected each of the children who switched to a business account because FB-I made each of their contact details available in the HTML source code at the relevant times and also processed their contact information for a purpose that was intended only for traditional businesses at the time.

505. In assessing the level of damage suffered by the data subjects, I have had regard to the loss of control suffered by them over their personal data. Regarding transparency, Articles 12(1) and 5(1)(a) empower data subjects to make informed decisions about engaging with activities that cause their personal data to be processed, and making informed decisions about how to exercise their rights. A lack of transparency leads to a loss of control over personal data, which, in turn, results in damage to data subjects by restricting their ability to make decisions connected to the processing of their personal data. A core element of the principles of data minimisation and data protection by default in Articles 5(1)(c) and 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 a controller processes it in a manner that is not necessary in relation to the purposes of the processing.

506. FB-I’s infringement of Article 12(1) regarding the public-by-default processing prevented child users of Instagram from exercising control over their personal data. The lack of information in the registration process on the difference between public accounts and

private accounts, coupled with how there was no option to choose a private account when registering, inhibited those children from choosing to make their Instagram accounts private. While it was open to them to navigate the hyperlinks in the Data Policy in order to find out how to switch to a private account, the lack of information on the specific purpose of the default processing in the registration process and the Data Policy itself made it more difficult to understand the difference between public and private accounts and how to switch. By making it more difficult for children to make their accounts private, FB-I restricted their choice and denied them control over their personal data. I find that this loss of control represents a significant amount of damage to the data subjects.

507. I find that FB-I's infringement of Article 12(1) regarding the contact information processing also prevented child users of Instagram from exercising control over their personal data. The language used made it difficult for children to understand that a global audience of strangers would have access to their contact information if they switched to a business account. As a result, the language used by FB-I denied those children control over their personal data by preventing them from making an informed choice as to whether to switch to a business account. This created a much greater risk of inappropriate and inadvertent publication of contact details. I find that this loss of control represents a significant amount of damage to the data subjects.

508. I find that FB-I's infringement of Article 5(1)(a) also prevented child users of Instagram from exercising control over their personal data. It is clear from FB-I's submissions in this Inquiry that some business account users did not require the publication of their contact details. By failing to directly notify child users of business accounts that they were no longer required to publish their contact details, FB-I denied them the opportunity to consider that change and to exercise their rights accordingly. While this information was indirectly made available a number of weeks after the change (in the Help Centre Webpage and a blog post) it is clear that many data subjects, and in particular children, may not have seen that information. Therefore, FB-I denied those children control over their personal data. I find that this loss of control represents a significant amount of damage to the data subjects.

509. I find that FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the public-by-default processing also prevented the child users of Instagram from exercising control over their personal data. By imposing the public-by-default setting, FB-I processed the personal data of child users of Instagram, who may have wished to avail of a private Instagram profile, in a manner that went beyond what was necessary in relation to the purposes of the processing. 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. In the circumstances, the selection of the default mode of processing was made unilaterally by FB-I before children had the opportunity to restrict

access to their accounts, and likely before some of the children realised the default position. Therefore, this infringement restricted those children from exercising control over their personal data. I find that this loss of control represents a significant amount of damage to the data subjects.

510. I find that FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the contact information processing also prevented the child users of Instagram from exercising control over their personal data. By processing children's contact information publically, including in the HTML source code, FB-I extended the scope of the processing beyond what was necessary for the purposes of the processing. This processing also subjected the personal data to potential web scraping. This denied those data subjects control over their personal data by exposing it to potential mass collection in bulk by unauthorised third parties. I find that this loss of control represents a significant amount of damage to the data subjects.

511. In its submission of 9 August 2021, FB-I contends³⁶⁸ that the number of data subjects affected should be limited only to those data subjects whose personal data was processed by FB-I in a manner the user did not intend, and should not be based on the total number of monthly active child users. FB-I also contends that *"the number of data subjects affected can only be considered if that number can be linked to actual damage suffered"*, and further submits:

"Facebook Ireland does not consider there is a likelihood of a data subject suffering significant damage, in the circumstances of this case. Given that the Commission has not proven such damage, it is inappropriate to consider the number of data subjects in respect of the quantum of the fine"

512. I do not agree with FB-I in this regard. Article 83(2)(a) requires that due regard must be given to the level of damage suffered by data subjects. The WP29 Guidelines on Administrative Fines³⁶⁹ make clear that the imposition of a fine is not dependent on first establishing the precise level of damage that occurred, as follows:

*"If damages have been **or are likely to be suffered** due to the infringement of the Regulation then the supervisory authority should take this into account in its choice of corrective measure, although the supervisory authority itself is not competent to award the specific compensation for the damage suffered. The imposition of a fine is not dependent on the ability of the supervisory authority to establish a causal link between the breach and the material loss..."*
(emphasis added)

³⁶⁸ FB-I's submission of 9 August 2021, Annex A, paragraphs 15 to 17

³⁶⁹ WP29, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/67, WP 253, 3 October 2017, page 11

513. In assessing the level of damage for the purpose of Article 83(2)(a), it is therefore appropriate that I have regard to the likely level of damage suffered by data subjects (including non-material damage). Further to this, I do not agree that the number of data subjects can only be assessed cumulatively by reference to “*the actual damage*” suffered by data subjects. As the WP29 Guidelines make clear³⁷⁰, the number of data subjects involved is a relevant consideration because it tends to reveal whether an infringement was a systematic issue, or an isolated event. Accordingly, the number of data subjects, and the level of damage are two discrete considerations to be taken into account, and not linked in the manner suggested by FB-I. Accordingly, I do not accept FB-I’s submission that the DPC is limited to consideration of actual damage suffered by specific numeric classes of data subjects. This approach would unduly limit the DPC’s consideration of relevant matters. It is appropriate that I should have regard to likely damage suffered, and to the overall number of data subjects who were affected by the infringements.

514. I further do not agree with FB-I’s submission³⁷¹ that some child users may have understood the meaning and import of the processing, and should be discounted from the number of affected data subjects. In this regard, I note that the damage suffered by data subjects on this occasion is primarily related to a loss of control over processing, and the absence of appropriate risk assessment to ensure data protection rights. In my view, this damage was suffered by the full cohort of users who were prevented from exercising control over their personal data. It is not an adequate substitute for control that some of these child users could have ultimately made the same choices that FB-I implemented (regarding default processing or mandatory publication of certain personal data); such users were equally prevented from exercising well-informed control at a relevant time. Accordingly, I am satisfied that the above assessment of the number of data subjects affected and the level of damage suffered by them is appropriate in the circumstances.

M.1.A The nature of the infringements

515. The nature of both of FB-I’s infringements of Article 12(1) concern data subjects’ right to information about the public-by-default processing and the contact information processing. Article 12(1) sets out the manner in which controllers must communicate the information referred to in Articles 13 and 14 to data subjects. If controllers do not communicate that information in a manner that complies with Article 12(1), data subjects may be denied an understanding of how their personal data is processed. It follows that these infringements of Article 12(1) concern data subjects’ right to information. This is a cornerstone of the rights of the data subject. The provision of information in a “*concise, transparent, intelligible and easily accessible form, using clear and plain language*” goes to the very heart of the fundamental right of the individual to

³⁷⁰ Ibid, page 10

³⁷¹ FB-I’s submission of 9 August 2021, Annex A, paragraph 15

protection of their personal data, which stems from the free will and autonomy of the individual to share his/her personal data in a voluntary situation such as this. Article 12(1) emphasises the importance of the requirements *“in particular for any information addressed specifically to a child”*. Where an infringement of Article 12(1) concerns information provided to children, that infringement is even more likely to deny those data subjects an understanding of the processing and the risks associated with it.

516. Articles 83(4) and (5) GDPR are directed to the maximum fine that may be imposed in a particular case. The maximum fine prescribed by Article 83(5) GDPR is twice that prescribed by Article 83(4) GDPR. The infringements covered by Article 83(5) GDPR include infringements of the data subject’s rights pursuant to Article 12 to 22 GDPR and infringements of the principles in Article 5 GDPR. It is therefore clear that the legislator considered the data subject rights and the data protection principles in Article 5 to be particularly significant in the context of the data protection framework as a whole. This is one factor to consider when assessing the nature of the infringements.

517. I have also assessed the nature of FB-I’s infringement of Article 12(1) regarding the public-by-default processing in light of the nature and scope of this processing. The nature of this processing concerns the publication of children’s social media content on Instagram publically by default. The scope concerns that publication to an indefinite and unrestricted audience. FB-I’s infringement of Article 12(1) likely denied children an understanding of this nature and scope. Accordingly, this lack of transparency likely affected children’s decisions when registering for Instagram accounts. It also likely affected their decisions on the personal data that they shared on their accounts after registering. I find that the nature of this infringement of Article 12(1) is most serious in nature.

518. I have also assessed the nature of FB-I’s infringement of Article 12(1) regarding the contact information processing in light of the nature and scope of this processing. The nature of this processing entails publishing children’s contact information on their Instagram business accounts. The scope concerns that publication to an indefinite and unrestricted audience. FB-I’s infringement of Article 12(1) likely denied children an understanding that, by switching to a business account, their phone numbers or email addresses would become publically available to this indefinite and unrestricted audience. The lack of clear and plain language in this regard likely affected children’s decisions to switch to business accounts. I find that the nature of this infringement of Article 12(1) is most serious in nature.

519. The nature of FB-I’s infringement of Article 5(1)(a) concerns its failure to notify existing users of the change in purposes of the contact information processing when FB-I removed its requirement that child users publish their contact information. Hence, the infringement goes to the autonomy of child users of Instagram business accounts to consider the nature of this change and to exercise their rights under the GDPR

accordingly. This infringement likely prevented those children from understanding that they could take action to prevent their contact details being published to an indefinite and unrestricted audience on their business accounts. This likely affected those users' decisions regarding the ongoing processing of their contact information. I find that the nature of FB-I's infringement of Article 5(1)(a) is serious.

520. The nature of FB-I's infringements of Article 35(1) concern its failure to conduct DPIAs in respect of the public-by-default processing and the contact information processing respectively. DPIAs are important tools for assessing risks to data subjects and for identifying measures to address those risks. The nature of both of FB-I's infringements of Article 24(1) concern its failure to implement appropriate measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. The nature of both of FB-I's infringements of Article 25(1) concern its failure to implement appropriate measures designed to implement the data-protection principles in an effective manner; and to integrate the necessary safeguards. Hence, the nature of FB-I's infringements of Articles 35(1), 24(1) and 25(1) all relate to FB-I's failure to identify and to implement appropriate measures in respect of the public-by-default processing and the contact information processing in order to ensure and demonstrate compliance with the GDPR and to protect the rights of the data subjects. Having regard to the nature and scope of the public-by-default processing and the contact information processing respectively, I consider that this failure to implement appropriate measures to ensure and demonstrate compliance and to mitigate the risks posed by each of the processing operations is serious. Therefore, I consider that the nature of FB-I's infringements of Articles 35(1), 24(1) and 25(1) is serious in respect of both the public-by-default processing and the contact information processing.

521. The nature of FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the public-by-default processing concern 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. FB-I's public-by-default audience setting for child users of Instagram resulted in their personal data being publically available to an indefinite and unrestricted global audience by default, even for children who may have wished to avail of private Instagram accounts. In light of the scope of the potential audience and the personal data that children may have shared before realising the default position or identifying how to restrict access to their account, I find that the nature of the infringements is serious.

522. The nature of FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the contact information processing concern 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. FB-I published the contact information of child users of Instagram business accounts even though the purpose of

that processing related only to traditional businesses until July 2019. FB-I also made the contact details of those children available in the HTML source code until November 2020 (but not between March 2019 and August 2020) even though this was not necessary in order to facilitate business users in providing contact details to customers. Hence, these infringements resulted in FB-I processing children's contact information in a manner that went significantly beyond what was necessary for the purposes at the time. I find that the nature of these infringements is serious in light of how they resulted in the unlawful publication of children's contact information to indefinite and unrestricted audience, including in the HTML source code format.

523. In its submission of 9 August 2021, in response to the PDD, FB-I contends³⁷² that the DPC's findings are based on novel interpretations of the law, which have not been notified to FB-I on a prior basis, and which are not explicitly found in the GDPR. In this regard, I note that the GDPR is directly effective and requires accountability and responsibility for processing on the part of controllers; a controller is not entitled to regulatory forbearance in respect of its obligations solely on the basis that novel applications of the law are involved. Further to this, the GDPR is principles-based, and not a prescriptive set of rules on processing; the lack of "explicit" legislative provisions is an inherent and intentional aspect of the Regulation. Accordingly, FB-I cannot reasonably expect a less than rigorous application of the GDPR solely on the basis that the law does not prescribe concrete actions that apply to the specific processing at issue. FB-I's obligations in terms of transparency, risk assessment, and data protection by design and default apply irrespective of the need for additional guidance or input from third parties. FB-I also reiterates its objections to the DPC's findings regarding Article 12(1) in this context, and submits that even if appropriate measures were not taken in respect of the mode of provision of information, weight should be given to the fact that direct links to information were provided. I am satisfied however, having considered in detail (in Part F of this Decision) the partial measures implemented by FB-I regarding the provision of relevant information, that the infringements in question have been properly considered above for the purposes of Article 83. Finally, FB-I contends (by summary comparison to other decisions made by the Dutch Data Protection Authority and the DPC) that the within infringements should be regarded as less serious. In this regard, I do not agree with FB-I's apparent view that comparisons of fines levied by supervisory authorities in differing circumstances is an appropriate or accurate way to assess the nature of GDPR infringements. As can be seen from the detailed analysis of processing on this occasion, a decision on the nature of an infringement requires an in-depth and fact specific assessment of processing of personal data by a controller. I also note that Articles 58(2)(i) and 83(2) each expressly state that administrative fines depend on the circumstances of

³⁷² FB-I's submission of 9 August 2021, paragraphs 132 to 135 and Annex A, paragraphs 1 to 5

the individual case. Accordingly, I am not convinced by the direct comparative approach suggested by FB-I.

M.1.B The gravity of the infringements

524. 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 public-by-default processing and the contact information processing to the rights and freedoms of child users of Instagram. These risks include the severe risk that dangerous individuals may communicate directly with child users of Instagram. I have outlined above that I agree with FB-I's assessment (as set out in the LIA) that such communication could result in *"grooming; physical, sexual and emotional abuse; [and/or] trafficking"*. The risks also include the possibility of contact information in HTML being targeted for web scraping, giving rise to a significant risk of fraud and impersonation. The fact that FB-I's infringements increased those risks to child users of Instagram goes directly to the gravity of those infringements. The GDPR's objectives include protecting the fundamental rights and freedoms of natural persons³⁷³. 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 that the manner in which FB-I's infringements increased the risks posed to child users of Instagram is highly relevant when assessing the gravity of those infringements.

525. In assessing the gravity of FB-I's infringement of Article 12(1) regarding the public-by-default processing, I have had regard to how the infringement affected [REDACTED] children. I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those children from exercising control over their personal data. Finally, I have also had regard to how the infringement increased the risks posed by the public-by-default processing to the rights and freedoms of the data subjects. In ordinary circumstances, children may be less aware of the risks, consequences and safeguards in relation to the processing of their personal data. However, FB-I's infringement of Article 12(1) significantly increased the likelihood that children would not understand the difference between public and private accounts. FB-I's infringement also increased the likelihood that children would not understand that their accounts were set to public by default and that this could only be changed after registering for a public account. This meant that child users were less likely to make informed decisions on the content of their public posts, for example, when deciding

³⁷³ Article 1(2) of the GDPR.

whether to share personal data that may be sensitive, such as location data. By denying children information in a clear and transparent form, these children were less likely to understand the risks of the public-by-default processing. Therefore, they were less likely to understand that there was a risk of contact from strangers and were less likely to take steps to mitigate against that risk. This infringement of Article 12(1) increased the risks posed by the public-by-default processing to the rights and freedoms of the child users of Instagram. I find that the gravity of this infringement is highly serious.

526. In assessing the gravity of FB-I's infringement of Article 12(1) regarding the contact information processing, I have had regard to how the number of data subjects affected is lower than the number affected by the public-by-default processing. Nonetheless, the infringement affected hundreds of thousands of child users in the European Region (approximately one in twenty child users). I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those children from exercising control over their personal data. I have also had regard to how the infringement increased the risks posed by the contact information processing to the rights and freedoms of the data subjects. Publishing children's phone numbers and email addresses to an indefinite and unrestricted audience creates a risk of off-platform contact from dangerous individuals. Tools implemented by Instagram to safeguard the activities of children on the platform would not cover any off-platform contact. This processing also created the further risk of fraud and impersonation. These risks are inherent to the public processing of children's contact information and FB-I's infringement of Article 12(1) increased these risks. The lack of clear and plain language resulted in a situation where children switching to business accounts may not have been aware that a global audience of strangers beyond the knowledge or control of FB-I would have access to their contact details. Some users may not have had regard to the risks associated with this when deciding to switch and after switching. Therefore, child users may not have identified any link between that processing of their contact information and any subsequent contact actually received as a result. If child users of Instagram received off-platform contact from a dangerous individual, those children would be less likely to identify the dangerous nature of that contact if they were unaware that their contact information was available to an indefinite and unrestricted audience. While some Instagram users may have understood the consequences of providing this contact information, the lack of clear and plain language posed a particular risk to the rights and freedoms of the most vulnerable data subjects. Those children who did not understand the language used are also less likely to understand the potential risks of off-platform contact from strangers. For all of those reasons, I find that this infringement of Article 12(1) increased the risks posed by the contact information processing to the rights and freedoms of the child users of Instagram. I find that the gravity of this infringement is highly serious.

527. In assessing the gravity of FB-I's infringement of Article 5(1)(a), I have had regard to the number of data subjects affected, which is linked to the number of data subjects affected by FB-I's infringement of Article 12(1) in respect of the contact information processing. This infringement also resulted in damage to child users of Instagram business accounts, specifically by preventing them from exercising control over their personal data by denying them the opportunity to consider the change and to exercise their rights accordingly. The infringement of Article 5(1)(a) prevented children, who would have opted to remove their contact details, but were not aware that it was no longer a requirement to publish the contact details, from removing that contact information. Therefore, this prevented those data subjects from taking a step to mitigate the risk posed to their rights and freedoms by the contact information processing. In those circumstances, I find that the gravity of this infringement is serious.

528. I have assessed the gravity of FB-I's infringements of Articles 35(1), 24(1), and 25(1) in light of how these infringements resulted in FB-I's failure to identify and to implement appropriate measures in respect of the public by the default processing and the contact information processing to ensure and demonstrate compliance with the GDPR and to protect the rights of the data subjects. By failing to implement appropriate measures, FB-I increased the risk posed by the public-by-default and the contact information processing to the rights and freedoms of those data subjects. For example, regarding the public-by-default processing, appropriate measures may have included a technical measure that prevented adults from sending messages to children who don't follow them (as implemented by FB-I in March 2021). The absence of this measure or other appropriate measures at the time under consideration clearly increased the risk of contact between dangerous individuals and children on the platform. Regarding the contact information processing, the absence of appropriate measures increased the risk of off platform contact between dangerous individuals and child users. I have also had regard to the high number of data subjects affected by the infringements of the public-by-default processing and the contact information processing respectively (as outlined above). For those reasons, I find that the gravity of FB-I's infringements of Articles 35(1), 24(1), and 25(1) regarding both the public-by-default processing and the contact information processing is serious.

529. In assessing the gravity of FB-I's infringements of 5(1)(c) and 25(2) regarding the public-by-default processing, I have had regard to how FB-I set the accounts of all of the child users of Instagram in the European Region to public without first giving those data subjects a choice between public and private accounts. Therefore, these infringements affected [REDACTED] data subjects. I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those children from exercising control over their personal data. These infringements also increased the risk posed to the rights and freedoms of those data subjects. FB-I processed the personal data of child users of Instagram, who may have wished to avail of a private

Instagram profile, in a manner that went beyond what was necessary in relation to the purposes of the processing. This processing made children's accounts available to an indefinite and unrestricted global audience before they had the chance to amend the setting and before some users likely realised that their accounts were public. As this processing was not necessary for its purpose at the time, the infringement is directly linked to creating the risk of contact between dangerous individuals and child users of Instagram who wished their accounts to be private. In those circumstances, I find that the gravity of FB-I'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.

530. In assessing the gravity of FB-I's infringements of Article 5(1)(c) and 25(2) regarding the contact information processing, I have had regard to how these infringements resulted in the unnecessary publication of the contact information of child users of Instagram business accounts to an indeterminate global audience until July 2019. As this processing was not necessary for its purpose at the time, the infringement is directly linked to creating the risk of off platform contact between dangerous individuals and child users of Instagram business accounts. I have also had regard to how the unnecessary processing in the HTML source code created the specific risk of web scraping and, consequently, the risk of fraud and impersonation. As set out above, the infringements affected a significant number of data subjects. I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those children from exercising control over their personal data. For all of these reasons, I find that the gravity of these infringements is serious.

531. In its submission of 9 August 2021, FB-I reiterates its views³⁷⁴ that the DPC's findings are based on hypothetical risks, which have not been balanced appropriately against the benefits of the Instagram service for child users. In this regard, I refer to the detailed treatment of these issues in Part G above. FB-I also contends that "loss of control" as a form of harm should be limited to situations where there has been a data breach, as described in Recital 85 GDPR. FB-I suggests therefore that "loss of control" is not relevant to the present circumstances as a form of harm. In this regard, FB-I fails to take into consideration the risks to the rights and freedoms of natural persons as described in Article 75 GDPR, which include the risk that *"data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data"* (emphasis added). I am therefore satisfied that it is appropriate to consider such a loss of control in the present context, and not only in relation to situations involving data breaches. FB-I also asserts that a loss of control should not be considered a form of "damage" for the purpose of the GDPR. I am satisfied that Recital 75 GDPR comprehends loss of control as a form of damage under the GDPR. I am also satisfied that it is not necessary for the DPC to identify individual data subjects affected as the only form of

³⁷⁴ FB-I's submission of 9 August 2021, paragraphs 136 to 139 and Annex A paragraphs 6 to 13

acceptable evidence of damage. The DPC must also consider likely damage to data subjects based on the facts, as made clear in the WP29 guidelines and set out above. With regard to the public-by-default processing, FB-I contends that the third party sources referred to by the DPC in this Decision are not applicable to the facts of this Inquiry, and have otherwise been misconstrued by the DPC. In this regard, I am satisfied that the DPC assessment of processing in Part G of this Decision is based on relevant factual considerations, as set out therein. With regard to the contact information processing, FB-I asserts that the DPC has not identified “concrete examples” of harm occurring in this context. For reasons which are set out above, and as set out in the WP29 Guidelines, the DPC is satisfied that consideration of risk and damage does not require the DPC to establish direct causal links to actual damage to specific individual data subjects. The DPC also refers to the treatment of this risk in Part G of this Decision.

M.1.C The duration of the infringements

532.FB-I’s infringement of Article 12(1) regarding the public-by-default processing commenced at the application of the GDPR on 25 May 2018. FB-I carried out the public-by-default processing before that date and failed to provide child users of Instagram with information on the purposes of the processing in a clear and transparent form. In the circumstances, it is clear that this infringement was ongoing at the commencement of this Inquiry on 21 September 2020. I acknowledge that, on 16 March 2021, FB-I introduced a new process that gives child users the option to choose between a public or private account when signing up for Instagram. 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 this infringement under Article 12(1) GDPR lasted at least from 25 May 2018 until the commencement of the Inquiry on 21 September 2020.

533.FB-I’s infringement of Article 12(1) regarding the contact information processing also commenced at the application of the GDPR on 25 May 2018. From at least February 2018, FB-I required child users of business accounts to display their contact information and failed to provide those users with information using clear and plain language on the purposes of the processing and information on the categories of recipients of personal data. On 4 September 2019, FB-I removed its mandatory requirement for child users of Instagram to display contact information when switching to a business account. I have set out above my finding that the information provided by FB-I after 4 September 2019 in the course of the business account switching process was in compliance with Article 12(1). 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 the Article 12(1) GDPR commenced on 25 May 2018, and ended on 4 September 2019.

534. The duration of FB-I's infringement of Article 5(1)(a) commenced on 4 September 2019 when it removed its mandatory requirement that child users publish contact information but did not directly notify existing child users of Instagram business accounts. The infringement was ongoing at the commencement of this Inquiry on 21 September 2020 because FB-I had not directly notified those child users at that date. Therefore, the infringement lasted at least from 4 September 2019 until the commencement of the Inquiry on 21 September 2020.

535. Regarding the duration of FB-I's infringements of Article 35(1), as outlined above, FB-I was undertaking the public-by-default processing and the contact information processing at the application of the GDPR on 25 May 2018. Article 35(1) does not have retrospective effect. However, as outlined above, the obligation to conduct assessments under Article 35(1) applied to FB-I by virtue of how those processing operations remained under frequent review and amendment by FB-I since the application of the GDPR and in line with the ongoing nature of the obligations under Article 35(1). Therefore, for the purposes of this Decision, I find that each of these infringements was ongoing as of 25 July 2018. In the circumstances, I consider that FB-I ought to have conducted assessments under Article 35(1) within 2 months of the GDPR's application in line with the ongoing nature of the obligation in Article 35(1) and in keeping with FB-I's general accountability requirements. Therefore, for the purposes of deciding whether to impose administrative fines, and for calculating the appropriate amounts if applicable, the DPC proceeds on the basis that the infringements under Article 35(1) GDPR commenced on 25 July 2018. The infringements were ongoing at the commencement of this Inquiry on 21 September 2020 because the processing operations were ongoing at that stage and FB-I had not undertaken the DPIAs. 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 infringements under the Article 35(1) GDPR commenced on 25 July 2018 and ended on 21 September 2020.

536. The duration of FB-I's infringements of Articles 24(1) and 25(1) regarding the public-by-default 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. These infringements were ongoing at the commencement of this Inquiry on 21 September 2020. 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 these infringements under Article 24(1) and 25(1) GDPR lasted at least from 25 May 2018 until the commencement of the Inquiry on 21 September 2020.

537. The duration of FB-I's infringements of Articles 24(1) and 25(1) regarding the contact information processing also commenced at the application of the GDPR on 25 May 2018. While FB-I removed its mandatory requirement that child users publish contact

information when switching to a business account on 4 September 2019, it still carries out this processing on an optional basis. I find that these infringements were ongoing at the commencement of this Inquiry on 21 September 2020 in circumstances where FB-I has not demonstrated its compliance with its obligation to implement appropriate measures in respect of its ongoing contact information processing. 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 these infringements under Articles 24(1) and 25(1) GDPR lasted at least from 25 May 2018 until the commencement of the Inquiry on 21 September 2020.

538. The duration of FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the public-by-default processing commenced at the application of the GDPR on 25 May 2018. FB-I's practice of making Instagram accounts public by default was in place prior to that date. Therefore, it failed to ensure that its processing of children's personal data was limited to what was necessary for their purposes from then. This infringement was ongoing at the commencement of this Inquiry on 21 September 2020. 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 these infringements under Articles 5(1)(c) and 25(2) GDPR lasted at least from 25 May 2018 until the commencement of the Inquiry on 21 September 2020.

539. The duration of FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the contact information processing commenced at the application of the GDPR on 25 May 2018. FB-I published the contact details of child users of Instagram as early as 2016 when business accounts were first created. It also made the contact details available in the HTML source code prior to the GDPR's application. In July 2019, FB-I changed the purpose of this processing to encompass the on-platform professional activities of new types of professional Instagram users. Therefore, this part of the infringements ended in July 2019. However, FB-I continued to make the contact details of child users available in the HTML source intermittently until November 2020 despite this not being necessary for the purposes of the processing. Therefore, FB-I was infringed Articles 5(1)(c) and 25(2) regarding the contact information processing until November 2020. On the face of it, the duration of these infringements was from 25 May 2018 to November 2020. However, FB-I removed the phone numbers and email addresses from the HTML source code for a time between March 2019 and August 2020. Furthermore, as FB-I changed the purpose of the processing to encompass the on-platform professional activities of new types of professional Instagram users from in July 2019, it is clear that neither part of the infringements was present between July 2019 to August 2020. Therefore, I find that the duration of these infringements does not include the period between July 2019 to August 2020.

540. In its submission of 9 August 2021, FB-I contends that the duration of the infringements *“cannot be a factor that either warrants the imposition of an administrative fine or increases the amount of any such fine given the standards the Commission is seeking to impose are not reflected directly in the GDPR and only became known to [FB-I] once the Draft Fundamentals was published and on receipt of the PDD”*. I do not agree with FB-I in this regard. As has been set out at the outset of this Decision in Part D, FB-I was obliged to be responsible and accountable for its processing since the outset of the GDPR, which has direct effect. The findings set out in this Decision are specific to processing by FB-I, and not based on the application of draft DPC guidance. FB-I also submits that the timing of certain service modifications after the commencement of the Inquiry should be taken into account for the purpose of Article 83(2). In this regard, I note that the DPC assessment of duration refers to the temporal scope of this Inquiry, which is limited to the period between the application of the GDPR in 2018, and the commencement of the Inquiry. I am therefore satisfied that I have correctly taken the duration of the infringements into account above, in a manner which clearly identifies the specific periods of processing which are relevant.

Assessment of the Article 6(1) infringement for the purpose of Article 83(2)(a)

541. In relation to the finding of infringement of Article 6(1) GDPR, I have assessed the Article 83(2)(a) criteria by reference to the views that have been expressed by the EDPB (in the Article 65 Decision) and the Norwegian SA (in the Objection), as outlined below.

542. In considering the nature, gravity and duration of the infringement, I have had regard to the analysis in Part G.1 of this Decision concerning the nature, scope and purposes of the contact information processing. Article 83(2)(a) GDPR requires these matters to be taken into account in having regard to the nature, gravity and duration of the infringements.

543. As regards the nature of the infringement, paragraph 239 of the Article 65 Decision records the EDPB’s view that:

“The EDPB reiterates that lawfulness of processing is one of the fundamental pillars of the data protection law and considers that processing of personal data without a legal basis is a clear violation of the data subjects’ fundamental right to data protection.”

544. The Norwegian SA, at page 8 of the Objection has further expressed the view that:

“the principle of lawfulness enshrined in Article 5(1)(a) GDPR and further specified in Article 6(1) is a fundamental pillar of the GDPR.”

545. It is therefore clear that both the EDPB and NO SA consider the infringement to concern one of the “fundamental pillars” of the GDPR.

546. As regards the gravity of the infringement, the Norwegian SA, at page 8 of the Objection, has expressed the view, in this regard, that:

“The processing of personal data of children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.”

547. I further note that infringements of Article 6 are subject to the higher fining threshold set out in Article 83(5) GDPR. As already reflected in paragraph 516 of this Decision, this arrangement clearly indicates that the legislator considered the matters covered by Article 83(5) GDPR to be particularly significant in the context of the data protection framework as a whole.

548. It is therefore clear that the infringement of Article 6(1) GDPR concerns a matter of significant gravity, noting the EDPB’s and the Norwegian SA’s reflections concerning the requirement for specific protection where the processing concerns the personal data of children (noting also the provisions of Recital 38 GDPR). I further note the Norwegian SA’s particular reference to the requirement for such specific protection in cases where the processing is carried out for the purposes of creating personality or user profiles and the collection of personal data relating to children in the context of services offered directly to a child.

549. As regards the duration of the infringement, paragraph 239 of the Article 65 Decision records the EDPB’s view that:

“... the identified infringement lasted at least from 25 May 2018 until the commencement of the IE SA’s inquiry in the present case on 21 September 2020.”

550. It is therefore clear that the infringement occurred over a limited but lengthy period of time.

551. As regards the number of data subjects affected, paragraph 239 of the Article 65 Decision records that:

“the EDPB recalls that the infringement at issue relates to the processing of personal data of a significant number of children”

552. In expressing the above view, the EDPB referred to paragraph 489 of the Draft Decision (now paragraph 503 of this Decision), which records that the number of data subjects affected by the findings of infringement concerning the contact information processing (the processing underlying the EDPB’s finding of infringement of Article 6(1) GDPR):

“is likely to be significant, in light of the fact that there are currently [REDACTED] child users with business accounts.”

553. This Decision notes, in this regard, that:

“While it is possible that fewer child users operated business accounts at the relevant times, I also note that many child users would probably have been diverted to the alternative “creator account” after July 2019. I am satisfied that the processing was likely to have affected hundreds of thousands of children. It is therefore obvious that there was a very significant number of child users that switched to professional accounts, and in particular, hundreds of thousands of children switched to a type of account that was intended for traditional businesses.”

554. The Norwegian SA, at page 8 of the Objection has expressed the view, in this regard, that:

“The number of data subjects affected in the EEA amounts to at least ... [REDACTED] users for the contact information processing.”

555. It is therefore clear that the infringement affected a large number of data subjects.

556. As regards the level of damage suffered by the data subjects in question, paragraph 239 of the Article 65 Decision records that:

“the EDPB recalls that the infringement at issue relates to the processing of personal data of a significant number of children and that the level of damage affected them has to be considered”

557. In expressing the above view, the EDPB referred to paragraphs 499 and 500 of the Draft Decision (now paragraphs 513 and 514 of this Decision). The relevant damage, as assessed in paragraphs 513 and 514 of this Decision, concerns the loss of control over processing. It is important to note, in this regard, that, at paragraph 512(2) of this Decision, I concluded, further to my assessment of the relevant matters arising, that *“the loss of control over personal data constitutes significant damage in the circumstances.”*

558. The Norwegian SA, at page 8 of the Objection, has expressed the view, in this regard, that:

“The damage suffered is intangible, but it would be safe to assume that the unlawful processing activities had a considerable and detrimental impact on the data subject’s digital lives.”

559. It further expressed the view that:

“Processing personal data without a legal basis is a clear violation of the data subjects’ fundamental right to data protection, because no one should have to

tolerate processing of their personal data save for when it is legitimised by the legislators.”

560. It is therefore clear that the EDPB and NO SA were agreed that the damage suffered by the data subjects was significant, comprising loss of control over personal data.

561. On the basis of the views that were expressed by both the Norwegian SA and the EDPB, as recorded above, I proposed to conclude that the infringement of Article 6(1) GDPR falls within the upper range of the scale, in terms of seriousness, for the purpose of the assessment of the Article 83(2)(a) criterion.

562. In its Final Submissions, FB-I disagreed³⁷⁵ with the above assessment and conclusion. In terms of the assessment of the nature of the infringement, FB-I submitted that:

- a. It relied in good faith on legal bases that it believed applied to the processing at issue and discharged its accountability obligations;
- b. the DPC, at least provisionally, agreed with FB-I and initially found no infringement of Article 6(1) GDPR; and
- c. the Article 65 Decision did not reach definitive findings on important aspects of the tests applicable under Article 6(1) GDPR.

563. While acknowledging FB-I’s submissions, above, such matters are not relevant to the assessment of the nature of the infringement.

564. In terms of the duration of the infringement, FB-I submitted that “*limited*” is the proper description to be applied to the duration of the infringement. I have already acknowledged, in my assessment, that the duration of the infringement was “*limited*”. The fact remains, however, that, while “*limited*” in duration, the infringement nonetheless occurred over the course of a period of at least two years. Regardless of what descriptive term is used to describe this period of time, the factual reality is that a period of at least two years is a lengthy period of time and must be taken into account when assessing this aspect of matters.

565. In terms of the assessment of the level of damage suffered by the data subjects, FB-I disagreed with the assessment on the basis that:

- a. The assertions regarding “loss of control” giving rise to “significant” damage are not supported by evidence;
- b. The DPC itself did not find an infringement of Article 6(1) and not all CSAs objected to the DPC’s approach; and

³⁷⁵ The Final Submissions, paragraphs 6 to 12, inclusive

- c. This Decision records, further below, that FB-I made significant changes to the contact information processing and the public by default processing, which, in any event, mitigated the alleged damage to data subjects.

566. The matters summarised at points b. and c., above, are not relevant to the assessment of the level of damage suffered by the data subjects. As regards the submissions summarised at a., above, it is firstly important to remember that the DPC is subject to a binding decision of the EDPB that indicates includes an endorsement not only of the views expressed by the Norwegian SA, as regards the damage suffered by the data subjects concerned, arising from the infringement of Article 6(1) GDPR, but also a requirement for the DPC to assess the damage suffered by reference to the damage that has already been outlined at paragraphs 513 and 514, above, i.e. loss of control. In the circumstances, it is not open to the DPC to conclude, as appears to be suggested by FB-I in its Final Submissions, that no harm was suffered by the data subjects concerned.

567. As regards the submissions that concern the lack of evidence to support any such considerations, there is no requirement for me to demonstrate “evidence” of damage to data subjects as part of my assessment of the Article 83(2) criteria. Were it otherwise, data protection authorities would only be able to carry out a full assessment of the Article 83(2) criteria in complaint-based inquiries which would permit the interrogation of individual data subjects for the purpose of adducing “evidence” of damage suffered as a result of a given infringement. As a statutory regulator carrying out functions pursuant to the GDPR and the 2018 Act, the Commission is well placed and uniquely qualified to assess the damage caused by a given infringement for the data subjects concerned. The same applies to the DPC’s co-decision-makers, such as the Norwegian SA and the EDPB itself, as regards their being equally well placed and uniquely qualified to assess the damage caused by a given infringement for the data subjects concerned. Otherwise, I note that I have already addressed similar submissions in paragraph 512, above. The views expressed in that paragraph apply equally here.

568. Accordingly, I remain of the view that, by reference to the views that have been expressed by both the Norwegian SA and the EDPB, as recorded above, the infringement of Article 6(1) GDPR falls within the upper range of the scale, in terms of seriousness, for the purpose of Article 83(2)(a).

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

569. 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 WP29 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.”³⁷⁶

570. 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.”³⁷⁷

571. 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.

572. 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.

573. FB-I’s infringement of Article 12(1) regarding the public-by-default processing concerns its failure to provide information concerning the purposes of this processing in a clear and transparent form. Hence, the characteristics of this infringement concern that lack of clarity and transparency in the information provided. In order to classify this infringement as intentional, I must be satisfied that (i) FB-I wilfully presented the information in the manner outlined and (ii) that it knew at the time that the information was not presented in a clear and transparent form. In making this determination, I must rely on objective elements of FB-I’s conduct that show the presence or absence of wilfulness and knowledge. While FB-I wilfully decided on the content of its registration stage and Data Policy, objective elements of FB-I’s conduct at the time suggest that this infringement was not intentional. At the relevant time, the Instagram Help Centre and other ancillary sources provided information that the accounts were public by default and information on how to switch. These sources were hyperlinked in the Data Policy. This objectively suggests that FB-I intended to provide this information with clarity and transparency and did not intend to deny child users of Instagram an understanding of the purposes of the processing, but rather unintentionally fell short of the standard required by presenting the information without the required clarity and transparency. Therefore, I find that this infringement was not intentional.

³⁷⁶ Article 29 Data Protection Working Party ‘Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679’ at page 11.

³⁷⁷ Ibid at page 12.

574. However, I find that FB-I's infringement of Article 12(1) regarding the public-by-default processing was negligent in the particular circumstances. Article 12(1) GDPR does not prescribe standard formats or practical arrangements when providing information. However, FB-I ought to have been aware that the information provided would not have been clear and transparent when viewed by child users. FB-I also ought to have been aware of the requirement for the Data Policy to provide explicit information on the specific purposes of the processing. In making this finding, I have had particular regard to how a company the size of FB-I ought to have been aware of its precise transparency obligations, in particular, in light of the quantity of children's data processed on the platform. I have also had regard to how the nature of FB-I's business entails processing large volumes of personal data. Therefore, I am satisfied that FB-I was negligent within the meaning of Article 83(2)(b).

575. FB-I's infringement of Article 12(1) regarding the contact information processing concerns its failure to provide information using clear and plain language concerning the purposes of that processing and the categories of recipients of the personal data. Hence, the characteristics of this infringement concern that lack of clear and plain language in the information provided. In order to classify this infringement as intentional, I must be satisfied that FB-I (i) wilfully presented the information in the manner outlined and (ii) that it knew at the time that the language used was not clear and plain. In making this determination, I must rely on objective elements of FB-I's conduct that show the presence or absence of wilfulness and knowledge. It is clear that FB-I wilfully decided on the content of its switching process and Data Policy. I have considered the language used in the switching process and Data Policy. This language was excessively general and made it difficult for children to understand that a global audience of strangers would have access to their contact information if they switched to a business account. However, I acknowledge that older Instagram users may have understood the consequences of providing their contact information in the circumstances. The language used does not suggest a deliberate attempt on the part of FB-I to avoid its obligations under Article 12(1) or knowledge that it was doing so, but rather that it fell short of the standard required, particularly when communicating with children. I do not find any objective elements of conduct that suggest that FB-I knew at the time that the language used was not clear and plain. While the language used fell significantly short of the standard required by Article 12(1), I find that this infringement was not intentional on the part of FB-I.

576. However, I find that FB-I's infringement of Article 12(1) regarding the contact information processing was negligent in the particular circumstances. There are [REDACTED] current child users with business accounts in the European Region, and it is therefore likely that at the relevant times, hundreds of thousands of child users were affected. It is clear that this created a duty on FB-I to ensure that the language used in its switching process and Data Policy was sufficiently clear and plain for those child users to

understand the intended category of recipients and the purposes of the contact information processing. In the circumstances, FB-I ought to have been aware at the time that the benign and positive way that they presented the contact information processing failed to meet the standard of what was required by Article 12(1) for communicating with children. In light of the extent to which FB-I processes children's data, it ought to have been aware of the defects in the language. Therefore, I am satisfied that FB-I was negligent within the meaning of Article 83(2)(b) in respect of this infringement.

577.FB-I's infringement of Article 5(1)(a) regarding the contact information processing concerns the fairness and transparency of its failure to notify existing child users of Instagram business accounts of its removal of its requirement that child users publish contact information. Hence, the characteristics of this infringement concern the fairness and transparency of the manner in which FB-I attempted to communicate this change to the relevant users by not directly notifying them. In order to classify this infringement as intentional, I must be satisfied that (i) FB-I wilfully decided not to directly notify those users and that (ii) FB-I knew that failing to do so was unfair and not transparent. In making this determination, I must rely on objective elements of FB-I's conduct that show the presence or absence of wilfulness and knowledge. FB-I actively decided to communicate the change in static sources of information a number of weeks after it implemented the change. I am satisfied that this objectively demonstrates that it wilfully decided to communicate the changes both in a delayed manner and in a manner that did not implement any direct notification method. FB-I's submission of 27 October 2020 objectively suggests that it was aware, prior to 4 September 2019, that some existing business account users did not have a business requirement to publish their contact information. By communicating the change late and only in static sources of information, I am satisfied that FB-I knew that some users would not be aware of this change as a result. In those circumstances, I find that FB-I knew that the lack of direct notification was unfair and not transparent in respect of those users. Therefore, I find that FB-I's infringement of Article 5(1)(a) was intentional because FB-I wilfully decided not to use direct notifications and knew that this was unfair and non-transparent in the circumstances.

578.FB-I's infringements of Article 35(1) in respect of the public-by-default processing and the contact information processing respectively concern its failure to conduct DPIAs in respect of each of those processing operations. The characteristics of these infringements concern a failure to conduct DPIAs in respect of processing operations that are likely to result in a high risk to the rights and freedoms of natural persons. In order for each infringement to be classified as intentional, I must be satisfied that (i) FB-I knew that the processing was likely to result in a high risk to the rights and freedoms of natural persons and (ii) that it wilfully omitted to carry out the DPIAs with that knowledge. FB-I's submission of 27 October 2020 stated that it did not conduct a DPIA in respect of the contact information processing because "*the processing is not likely to give rise to a high*

risk to the rights and freedoms of Teens”. Similarly, FB-I submitted that the risks of the public-by-default processing are not evident in circumstances where the processing takes place in the context of “*a safety-focused Instagram Service*”. However, FB-I’s LIA, submitted on 21 January 2021, objectively points to its knowledge that both processing operations result in a high risk to the rights and freedoms of child users of Instagram (although FB-I has subsequently sought to downplay these conclusions). This LIA also details how FB-I took the view that the measures implemented adequately mitigated that high risk. As outlined above, high-risk processing remains subject to Article 35 GDPR on an ongoing basis, regardless of steps taken by the controller to mitigate the risks. FB-I’s explanation for not carrying out a DPIA illustrates that it considered carrying out DPIAs and made a wilful decision not to. I am satisfied that its decision not to carry out DPIAs was wilful. Therefore, I find that both of FB-I’s infringements of Article 35(1) were intentional because FB-I had knowledge that the processing operations were likely to result in a high risk to the rights and freedoms of natural persons and it wilfully decided not to carry out DPIAs.

579. FB-I’s infringements of Articles 24(1) and 25(1) regarding the public-by-default processing and the contact information processing respectively concern its failure to implement appropriate measures: to ensure and to be able to demonstrate that the processing was performed in accordance with the GDPR; to implement data-protection principles in an effective manner; and to integrate the necessary safeguards into the processing. Hence, the characteristics of these infringements concern that lack of appropriate technical and organisational measures. In order to classify these infringements as intentional, I must be satisfied that (i) FB-I 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 Articles 24(1) and 25(1) respectively. Having considered the objective elements of FB-I’s conduct, I find no evidence that FB-I knew that its measures were not sufficient in respect of the public-by-default processing and the contact information processing at the time. Ordinarily, a DPIA that identifies measures, which a controller then failed to implement, would constitute an objective element of conduct that points to knowledge in respect of infringements of Articles 24(1) and 25(1). As outlined above, FB-I did not conduct DPIAs as required in respect of these processing operations, and these infringements of Article 35(1) were intentional. In those circumstances, it is also clear that FB-I ought to have been aware that it was falling short of the duty owed under Articles 24(1) and 25(1) because complying with Article 35(1) would have made FB-I aware of this. I find that FB-I’s failure to implement appropriate measures pursuant to Articles 24(1) and 25(1) in respect of both the public-by-default processing and the contact information processing was highly negligent in the circumstances.

580. FB-I’s infringements of Articles 5(1)(c) and 25(2) regarding the public-by-default processing concern 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. Hence, the characteristics of these infringements concern FB-I's failure to implement appropriate measures to ensure that the social media content of child users of Instagram 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) FB-I wilfully made child users' Instagram accounts public by default 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. In making this determination, I must rely on objective elements of FB-I's conduct that show the presence or absence of wilfulness and knowledge. I find that FB-I wilfully decided to make all Instagram accounts public by default, including children's Instagram accounts. It did not include any provision in the registration process to make an account private, but only included such options in the settings after registration. Furthermore, I find that FB-I knew at the time that this would result in processing that was not limited to what was necessary in relation to the purposes. FB-I's inclusion of a private option in the settings objectively illustrates at the time that FB-I knew that some data subjects used Instagram to share content with approved followers only. By making all accounts public by default, I find that FB-I knew that this would result in personal data processing that was not limited to what was necessary in relation to the purposes. Therefore, FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the public-by-default processing was intentional.

581. FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the contact information processing also concern 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. Hence, the characteristics of this infringement concern FB-I's failure to implement appropriate measures to ensure that it did not process the contact details of child users of Instagram business accounts prior to July 2019 in a manner that didn't comply with FB-I's own stated purpose that was intended only for traditional businesses; and its failure to implement appropriate measures to ensure that it did not process the contact details of child users of Instagram business accounts as plain text in the HTML source code. In order to classify this infringement as intentional, I must be satisfied that (i) FB-I wilfully processed children's contact details on business accounts prior to July 2019 and in the HTML source code, and (ii) that it knew at the time of this processing that it would result in personal data processing that was not limited to what was necessary in relation to the purposes. I find that FB-I wilfully processed children's contact details both on business accounts generally and in the HTML source code. FB-I stated that this processing was intentional on its part, and a necessary consequence of the children's decisions to publish their contact information to the world at large when switching to a business account. I find that FB-I knew that this processing was not limited to what was necessary in relation to the

purposes for some child users. The Facebook Security Team informed Mr Stier in March 2019 that the HTML processing was not necessary, yet FB-I continued to process it between August and November 2020. Therefore, as an organisation, FB-I knew that the processing was not necessary for its purposes. Furthermore, in circumstances where FB-I knew that children were utilising business accounts, and as a result, that FB-I was imposing a mandatory requirement on those children to display their contact details, it is clear that FB-I knew that its processing was not limited to what was necessary for its own stated purposes relating to traditional businesses. Therefore, I find that FB-I's infringements of Articles 5(1)(c) and 25(2) regarding the contact information processing were intentional.

582. In its submission of 9 August 2021, FB-I submits³⁷⁸ in respect of the above findings that the DPC should instead conclude that the infringements were the result of blameless inadvertence, and not negligent or intentional. In particular, FB-I contends that none of the infringements should be regarded as intentional on the basis that FB-I has: put in place functional teams regarding GDPR compliance and child users, engaged with the DPC and other relevant third parties, and has a privacy review process for new products and features. FB-I also contends that its service revisions since May 2018, and resourcing of a “cross-functional and cross-jurisdictional team” to address “youth-related regulatory requirements” are reflective of its actual intentions. FB-I submits that these measures *“are not indicative of an organisation that is intentionally breaching provisions of the GDPR”*, and that in the absence of detailed guidance to the contrary, it can be concluded that FB-I was a *“responsible controller”* acting in *“good faith”*. FB-I therefore appears to suggest that the *“intentional...character of an infringement”* depends on whether a controller formed a subjective view that the processing at issue would be contrary to the GDPR.

583. On balance, I am of view that that FB-I's intentions can also be objectively discerned by the character of the actions which constitute the GDPR infringement. FB-I may well have committed resources to the issue of child safety in the manner described. However, FB-I cannot claim that the infringements in question were merely “inadvertent” solely on the basis that it has otherwise implemented general organisational structures with the objective of GDPR compliance and child safety, or because it may have held a *“good faith”* belief that the processing was lawful. The infringements by FB-I are intentional (and not inadvertent) in the sense that the actions which constitute the infringements were done on purpose and deliberate; the controller expressly intended to publish the contact information of children (without a DPIA), and intentionally nudged new child users into public accounts (without a DPIA). These infringements were therefore intentional in character, because they involve wilful actions performed deliberately and in circumstances where the controller had prior knowledge of the nature of the

³⁷⁸ FB-I's submission of 9 August 2021, paragraphs 146 to 154

processing. While I accept that FB-I disputes the findings of infringement in this Decision, the character of these infringements was intentional.

584. FB-I also submits that the obligation to prepare a DPIA was unclear; I do not accept this submission in circumstances where the DPIA guidelines set out express criteria which apply to the processing at issue in this Inquiry.

585. Insofar that I have found that certain infringements by FB-I were negligent in character, FB-I contends³⁷⁹ that there is no basis for this finding, and states that the infringements are not similar to the examples of negligent processing set out in the Administrative Fines Guidelines³⁸⁰ (i.e. *“failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence”*). FB-I also asserts that the above infringements should not be regarded as negligent in circumstances where it was not provided with guidance on the application of the provisions at issue. In this regard, I am satisfied that the infringements in question were negligent in character, insofar that they constituted an unintentional breach of GDPR obligations on the part of the controller. I am further satisfied that *“good faith”* on the part of the controller, and the lack of additional legislative guidance do not alter the negligent character of the infringements. The GDPR places a high standard of accountability on controllers, and is not dependent on additional guidance to give full effect to data protection law. FB-I is therefore responsible for its actions which, although not intentional in character, fell short of the standard required under the GDPR, and were negligent in the sense that FB-I failed to take proper care to comply with its legal obligations.

586. On the basis of the foregoing, I am satisfied that my assessment of the intentional and negligent character of the infringements is appropriate in the circumstances of this Inquiry.

587. In relation to the finding of infringement of Article 6(1) GDPR, neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, and adopting the approach already reflected in paragraphs 571 and 572, above, I proposed to record a conclusion that the objective elements of conduct gathered from the facts of this case fall short of the threshold required to support a conclusion that the infringement of Article 6(1) GDPR was intentional in character. Accordingly, I proposed to conclude that the infringement of Article 6(1) GDPR fell to be classified as negligent for the purpose of Article 83(2)(b).

³⁷⁹ Ibid, Annex A paragraphs 20 to 24

³⁸⁰ Article 29 Data Protection Working Party ‘Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679’, page 12

588.FB-I, by way of the Final Submissions³⁸¹, disagreed with the above assessment and submitted that the Article 6(1) infringement ought to be classified as “merely inadvertent” on the basis that:

- a. FB-I relied in good faith on legal bases which the DPC itself considered could possibly be relied upon;
- b. During the relevant period, no specific regulatory guidance, interpreting provisions of the GDPR in the complex and multi-faceted context of youth-protection had been published by supervisory authorities or the EDPB;
- c. Where there is “a clear disagreement as to the correct interpretation of Article 6(1) GDPR – for example, where supervisory authorities themselves disagree as to the approach adopted and the EDPB is not definitive on key limbs of the relevant tests to be applied – it is not understood how the finding of infringement could be characterised as negligent.”

589. In relation to the submissions summarised at a. and b., above, I note that I have already addressed the potential impact of these matters on the assessment of the character of an infringement at paragraph 587, above. As regards the submissions summarised at c., above, I do not agree that it may be said that there is “a clear disagreement as to the correct interpretation of Article 6(1) GDPR”. The Article 65 Decision was adopted on the basis of a two-thirds majority of the members of the Board, in accordance with Article 65(2) GDPR. The views set out in the Article 65 Decision, including but not limited to the matters pertaining to the interpretation and application of Articles 6(1)(b) and (f) GDPR, represent the consensus position of the EDPB. The Article 65 Decision is further binding upon all CSAs, including the DPC. The assessments of the EDPB that resulted in, and support, the finding of infringement of Article 6(1) GDPR are simply not compatible with FB-I’s position that the Article 6(1) infringement is “*an inadvertent infringement and thus ought not to be the subject of an administrative fine at all.*” This is clear from the views that are set out in Section 5 of the Article 65 Decision, such as those set out in paragraphs 94 to 97 (inclusive) and paragraphs 124 – 126 (inclusive) thereof. Accordingly, I remain of the view that the infringement of Article 6(1) GDPR, as established by the EDPB, falls to be classified as negligent for the purpose of Article 83(2)(b).

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

590. I have found above that FB-I’s infringement of Article 5(1)(a) prevented child users of Instagram from exercising control over their personal data and that this represents a significant amount of damage to the data subjects. FB-I provided information on its removal of its requirement that child users publish contact information on Instagram

³⁸¹ The Final Submissions, paragraphs 13 – 15 (inclusive)

business accounts in the Instagram Help Centre webpage on 18 October 2019 and subsequently in a blog on 20 December 2019. While, these static sources of information were not sufficient for the purposes of Article 5(1)(a) and were provided a number of weeks after the change in processing was implemented, I consider that this action mitigated the damage suffered by some of the data subjects. This action likely made some of the data subjects aware of FB-I's removal of the requirement and, thus, mitigated the loss of control suffered by those data subjects. I find that this action is mitigating in respect of FB-I's infringement of Article 5(1)(a).

591. Throughout the Inquiry, FB-I has maintained that it did not infringe the GDPR in respect of the matters under consideration. Nonetheless, it has made significant changes to the contact information processing and the public-by-default processing (including changes made before and subsequent to the commencement of this Inquiry). FB-I's motivation for these changes was not to remedy the infringements because FB-I's position throughout the Inquiry is that it has not infringed the relevant provisions. Regardless of the motivation for the changes, I consider that the damage to data subjects has been mitigated by the following subsequent actions by FB-I:

- In the summer of 2019, FB-I implemented a second type of professional account on Instagram, known as a "creator account", as an alternative professional account to that used by traditional businesses. Users who opted for a creator account instead of a business account were not required to publish their contact information.
- From 4 September 2019 onwards, FB-I provided child users who were switching to a business account with information as required under Articles 12(1), 13(1)(c) and 13(1)(e) GDPR, in connection with the contact information processing.
- From 4 September 2019, FB-I made the contact information processing optional for users of business accounts.
- In November 2020 and for a time between March 2019 and August 2020, FB-I removed the phone numbers and email addresses from the HTML source code of Instagram profile webpages for child users.
- In January 2021, FB-I implemented a measure that allows child users to choose between a public and private account when registering for Instagram. These measures were further updated after the PDD, to ensure that the default audience setting is now "private".
- In January 2021, FB-I implemented a system of prompts which alert child users with public accounts of the audience setting.

- In March 2021, FB-I implemented a feature that prevents adults from sending messages to people under 18 who don't follow them.
- In March 2021, FB-I implemented a system of information prompts, in the form of safety notices, to warn child users when an adult who has been exhibiting potentially suspicious behaviour is interacting with them in direct messages on Instagram.
- Since April 2021, FB-I has begun to implement a new content filter for direct messages, and which allows users to create custom content filters for direct messages and comments. FB-I has also begun to implement a feature which prevents blocked users from making contact using alternative accounts.
- FB-I has implemented a cross-functional and cross-jurisdictional team to focus on youth-related regulatory guidance, and further implements teams and processes to combat unauthorised scraping of personal data (as described at Paragraph 98 of its submission of 9 August 2021).
- FB-I engages with external bodies and stakeholders on matters of child safety (as described at Paragraph 98).

592. While I consider that the above actions by the controller were mitigating in character, it is also the case that the damage caused on this occasion cannot be fully mitigated by the subsequent actions of FB-I; it is not always possible to retrospectively correct a past lack of control, as a data subject may already have suffered consequential damage as a result. This Decision does not make findings regarding the transparency of, or the appropriateness of the measures implemented in respect of, FB-I's ongoing processing of personal data that enables child users to create public accounts on a non-default basis following the changes implemented by FB-I in March 2021.

593. In its submission of 9 August 2021, FB-I submits³⁸² that greater weight should be attached to the above mitigating actions, in the context of assessing any administrative fine. In this regard, FB-I refers to two decisions of the DPC, in which the amount of a fine was reduced on the basis of mitigating actions taken by the controller. In the present circumstances, I must balance the serious nature of the infringements with the mitigating actions of the controller subsequent to the infringements. In this regard, I note that the above actions by FB-I may have mitigated the damage to data subjects after the infringements occurred for the purpose of Article 83(2)(c). Having regard to these actions for the purpose Articles 83(2)(c) (and including actions notified to the DPC subsequent to the PDD) I am of the view that the actions mitigated the damage to data subjects, and accordingly I have had regard to these actions when calculating the proposed administrative fine below.

³⁸² FB-I's submission of 9 August 2021, paragraphs 141 to 145, and Annex A paragraphs 25 to 28

594. In relation to FB-I's infringement of Article 6(1) GDPR, neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. I noted that FB-I's position, throughout this inquiry, has been one whereby it considered that it had appropriately assessed the obligations arising pursuant to Articles 6(1)(b) and 6(1)(f) such that the processing under examination was supported by a legal basis. Accordingly, and in circumstances where FB-I believed its processing operations to be lawful, I expressed the preliminary view that it would be unreasonable to expect FB-I to have taken action to mitigate the damage suffered by data subjects. Accordingly, I proposed to treat this factor as neither mitigating nor aggravating for the purpose of Article 83(2)(c).

595. FB-I, by way of the Final Submissions³⁸³, submitted that, in light of the various steps that it had taken to mitigate potential risks to data subjects, *"including as described in the legitimate interests assessment and [the] substantial voluntary modifications to Business Accounts, as detailed ... in relation to Article 83(2)(f) GDPR"*, I ought to take FB-I's actions into account as a mitigating factor under this heading. Consistent with my approach to similar submissions made in the context of the other infringements, I will take account of such matters as part of my assessment of the Article 6(1) infringement for the purpose of Article 83(2)(f). Accordingly, my views, for the purpose of the assessment required to be carried out pursuant to Article 83(2)(c) remains as set out in paragraph 587, above.

M.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;

596. 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."*³⁸⁴

597. I have found that FB-I infringed Articles 25(1) and 25(2) regarding both the public-by-default processing and the contact information processing. I consider that FB-I holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. It is clear that FB-I 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 FB-I, this factor cannot be considered aggravating in respect of the infringements. Rather, I must

³⁸³ The Final Submissions, paragraph 16

³⁸⁴ Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' at page 13.

independently consider pursuant to Article 83 whether these infringements of Article 25 merit the imposition of administrative fines in and of themselves.

598. In its submission of 9 August 2021, FB-I contends³⁸⁵ that it cannot be held accountable for retrospective standards, and states that “*due consideration must be afforded to the fact that neither the EDPB’s Article 25 guidance (finalised in October 2020) nor the Draft Fundamentals were available during the periods relevant to the Commission’s finding of infringement*”. I do not share FB-I’s apparent view that its GDPR obligations are contingent on the publication of additional guidelines and standards. FB-I was at all relevant times obliged to be responsible and accountable for the processing at issue, based on the provisions of the GDPR itself. I am therefore satisfied that the above conclusion on responsibility is accurate in the circumstances of this Inquiry.

599. In the context of the infringement of Article 6(1) GDPR, I note that neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, I proposed to conclude that the assessments recorded above would apply equally to the infringement of Article 6(1) GDPR.

600. FB-I, in the Final Submissions³⁸⁶, submitted that, for various reasons, this factor should be treated as neither aggravating nor mitigating. I note that, in conjunction with the proposed conclusion set out above, I made a corresponding proposal to treat my assessment under this heading as neither mitigating nor aggravating for the purpose of the Article 6(1) GDPR infringement. Given that this is the very conclusion sought by FB-I, in the Final Submissions, it is unnecessary for me to engage further with the matters addressed in this part of FB-I’s Final Submissions.

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

601. No relevant previous infringements arise for consideration in this context, including for the purpose of the finding of infringement of Article 6(1) GDPR that was established by the EDPB in the Article 65 Decision. FB-I has not sought, by way of the Final Submissions, to challenge this conclusion.

M.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;

602. Throughout the Inquiry, FB-I has maintained that it did not infringe the GDPR in respect of the matters under consideration. Nonetheless, it has made significant changes to the contact information processing and the public-by-default processing. FB-I’s motivation for these changes was not to remedy the infringements because FB-I’s position throughout the Inquiry is that it has not infringed the relevant provisions. Regardless of the motivation for the changes, I consider that FB-I is entitled to mitigation for this action

³⁸⁵ FB-I’s submission of 9 August 2021, Annex A paragraphs 29 and 30

³⁸⁶ The Final Submissions, paragraph 17

because it contributes towards remedying the infringements. In this regard, I refer to the mitigating actions set out above at Paragraph 591.

603. While I consider that these actions are mitigating and corrective of the adverse effects of the infringements, I also note that it is not possible to fully remediate the adverse effects on child users (in terms of the previous lack of control over personal data), because extensive processing may have occurred already in circumstances where child users were prevented from exercising control over their personal data. I make this finding without prejudice to the question of whether FB-I's on-going processing complies with the GDPR. In particular, as noted above, this Decision does not make findings regarding the transparency of, or the appropriateness of the measures implemented in respect of, FB-I's ongoing processing of personal data that enables child users to create public accounts on a non-default basis following the changes implemented by FB-I in March 2021.

604. In its submission of 9 August 2021, FB-I contends³⁸⁷ that the DPC should account for the extent to which mitigating factors have been taken into account when calculating fines. FB-I also submits that it remediated the infringements independently of the Inquiry process, and contends that the calculation of any administrative fine should take into account mitigating actions by FB-I. Having regard to these actions for the purpose Articles 83(2)(f) (and including the actions notified to the DPC subsequent to the PDD) I am of the view that the actions remedied the infringements to an extent, and mitigated the adverse effects of the infringement to an extent, and accordingly I have had regard to these actions when calculating the proposed administrative fine below.

605. In relation to FB-I's infringement of Article 6(1) GDPR, I note that neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, I proposed to conclude, for the purpose of the assessment required to be carried out for the purpose of Article 83(2)(f), that FB-I's position, throughout this inquiry, has been one whereby it considered that it had appropriately assessed the obligations arising pursuant to Articles 6(1)(b) and 6(1)(f) such that the processing under examination was supported by a legal basis. Accordingly, and in circumstances where FB-I believed its processing operations to be lawful, I proposed to conclude that it would be unreasonable to expect FB-I to have taken action (in cooperation with the DPC or otherwise) to remedy the infringement and mitigate the possible adverse effects of same.

606. FB-I, by way of the Final Submissions³⁸⁸, has submitted that my proposed approach is inconsistent with the other assessments carried out under this heading, whereby I indicated my intention to take into account the steps FB-I had taken to make changes to

³⁸⁷ FB-I's submission of 9 August 2021, Annex A, paragraphs 32 to 34

³⁸⁸ The Final Submissions, paragraphs 19 to 22 (inclusive)

the display of contact information for Business Accounts, on the basis that these actions remedied the relevant infringements to an extent. In the context of the Article 6(1) infringements, I note that the EDPB already considered the impact of the changes that were implemented by FB-I on 4 September 2019 and concluded that *“these elements are not sufficient to change the outcome of the balancing test”* in the context of processing based on Article 6(1)(f). As regards the submissions that I should also take account of the further changes made subsequent to FB-I’s submissions of 9 August 2021, I note that such changes post-dated the relevant period of infringement, as recorded as part of my assessment of Article 83(2)(a), above. In the circumstances, I remain of the view that it is appropriate for me to conclude that this aspect of matters ought to be treated as neither mitigating nor aggravating in the circumstances of the Article 6(1) infringement.

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

607. The categories of personal data affected by FB-I’s infringements of Articles 12(1), 35(1), 5(1)(c), 25(2), 25(1) and 24(1) regarding the public-by-default processing reflect the categories of personal data likely shared by children on public-by-default Instagram accounts. By setting children’s Instagram accounts to public by default, FB-I determined that the content of those accounts would be visible to an indefinite and unrestricted global audience. Therefore, it follows that FB-I’s infringements affected any categories of personal data likely shared on those public-by-default Instagram accounts.

608. It is not practicable for the purposes of this Inquiry to analyse the specific personal data actually shared by children on their public-by-default Instagram accounts. Instagram allows users to share their personal data through messages, audio, video calls and video chats, and by sending images and video files, including through public comments and conversations. FB-I estimates that there are ██████████ child users of Instagram in the European Region. FB-I submissions also described how *“People choose to join Instagram to share with a global community of diverse users, discover new content, and explore shared interests”*³⁸⁹. Furthermore, FB-I’s infringement of Article 12(1) risked denying children an understanding that their social media content would be visible to an indefinite and unrestricted audience. This, in turn, likely affected the categories of personal data that those children decided to share on those accounts, including categories of personal data intended for a more restricted audience of followers. In all the circumstances, I am satisfied that the categories of personal data likely shared by children on their public-by-default Instagram accounts include an extensive range of categories. This personal data shared is likely to include information on users’ daily lives and interests. The personal data may be sensitive as it may make a child user identifiable to dangerous persons due to the public processing of that personal data.

³⁸⁹ Submission dated 18 December 2020.

609. The categories of personal data affected by FB-I's infringements of Article 12(1), 5(1)(a), 35(1), 5(1)(c), 25(2), 25(1), and 24(1) regarding the contact information processing is significantly more narrow than the public-by-default processing. These categories are limited to children's email addresses and phone numbers. Therefore, it is necessary to consider the sensitivity of children's phone numbers and email addresses in the context of the contact information processing. I have outlined above the risk posed by the contact information processing. Publishing the contact information of child users of Instagram business accounts to an indefinite and unrestricted audience creates the risk of communication from dangerous individuals, and, as acknowledged by FB-I, this could result in "*grooming; physical, sexual and emotional abuse; [or] trafficking*". In light of these risks, I consider that the contact information of child users of Instagram business accounts is a highly sensitive category of personal data in the context of this processing.

610. In its submission of 9 August 2021, FB-I contends³⁹⁰ that the categories of personal data processed in the context of the public-by-default processing are "*limited*" and determined by the user. FB-I proceeds to suggest that, in the absence of a concrete assessment of the personal data of millions of child users, the categories of personal data affected must be regarded as a "*neutral*" factor when calculating the administrative fine. FB-I contends that the DPC's conclusions about the categories of personal data in relation to the public-by-default processing are "hypothetical" only, and not based on evidence. I do not agree with FB-I's submissions in this regard. There is a clear factual basis to demonstrate the fact that child users of Instagram are provided an open platform to share photographs, video and text, and to communicate with other users. 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.

611. In relation to infringement of Article 6(1) GDPR, I note that neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, I proposed to conclude that the assessment recorded at paragraph 609, above, applies equally to the infringement of Article 6(1) GDPR. On this basis, I proposed to conclude that the categories of personal data affected by the infringement of Article 6(1) are limited to the email addresses and phone numbers of child users and that, in light of the risks identified at paragraph 609, above, these categories of personal data constitute highly sensitive categories of personal data in the context of the processing in question.

³⁹⁰ FB-I's submission of 9 August 2021, Annex A, paragraphs 35 to 38

612. FB-I, by way of the Final Submissions³⁹¹, submitted that “*having regard to the very limited information that was subject to the processing ... and the absence of verifiable and/or expert evidence supporting a conclusion that the personal data involved in this case was in fact “highly sensitive” or the existence of actual harm*”, Article 83(2)(g) ought to be either considered to be a neutral factor or a factor that can only be given the lightest possible weight and have no material impact on the fine range proposed.

613. I note that the categories of personal data affected by the Article 6(1) infringement, and my proposed characterisation of those personal data, are the same as that reflected for the assessments of the other infringements that concern the contact information processing. I am satisfied that it is appropriate for me to treat the matters arising, for the purpose of the Article 6(1) infringement, in a manner that is consistent with the treatment afforded to the same matters in the context of the infringements reflected at paragraph 609, above.

M.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;

614. The infringements became known to the DPC as a result of the Breach Notification submitted by Mr David Stier on 17 June 2019 and the subsequent own-volition Inquiry conducted from 21 September 2020. The subject matter of the Inquiry did not give rise to any obligation on FB-I to make a formal notification to the DPC. FB-I contends³⁹² that the notification from Mr Stier should be regarded as a neutral consideration when calculating the administrative fine. In this regard, I note that there are mitigating actions in this context, to the extent that FB-I appears to have (temporarily) made changes to the HTML source code of profile pages following the Stier report. However, it is also the case that FB-I continued in the publication of on-platform contact information of child users after this issue was brought to their attention by Mr Stier. While I accept that FB-I subsequently made changes to this processing, its response to the Stier report was limited in terms of the extent of changes made at the time.

615. In relation to the infringement of Article 6(1), I note that neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, I proposed to conclude that the assessment recorded above – namely, that the subject matter of the inquiry did not give rise to any obligation on the part of FB-I to make a formal notification to the DPC – applies equally to the infringement of Article 6(1) GDPR. I note that FB-I has not objected, as part of its Final Submissions, to this approach. Accordingly, I remain of the review expressed above.

³⁹¹ The Final Submissions, paragraphs 23 and 24

³⁹² FB-I’s submission of 9 August 2021, Annex A, paragraph 39

M.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;

616. Corrective powers have not previously been ordered against FB-I with regard to the subject matter of this Decision. FB-I contends³⁹³ that its lack of prior infringements should be taken as a mitigating factor when assessing the fine. In circumstances where the principle of accountability obliges controllers to be responsible for the implementation of the GDPR, and where the GDPR has only been applicable since May 2018, I am of the view that the lack of previous measures ordered against FB-I is a slightly mitigating factor.

617. In relation to the infringement of Article 6(1) GDPR, neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, I proposed to conclude that the assessment recorded at paragraph 616, above, applies equally to the infringement of Article 6(1) GDPR. Accordingly, this will be treated as a slightly mitigating factor for the purpose of the Article 83(2) assessment. I note that FB-I's Final Submissions do not dispute this approach.

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

618. Such considerations do not arise in this case. Further to this, the absence of such codes or mechanisms is not a mitigating factor; FB-I was at all relevant times obliged to comply with the GDPR itself as a source of law, and failed to do so.

619. In relation to the Article 6(1) infringement, I note that neither the EDPB (in the Article 65 Decision) nor the Norwegian SA (in the Objection) have addressed this aspect of matters. In the circumstances, I proposed to conclude that the assessment recorded at paragraph 618, above, applies equally to the infringement of Article 6(1) GDPR. I note that FB-I has not sought, by way of the Final Submissions, to challenge this approach.

M.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.

620. I find that FB-I's infringement of Article 12(1) regarding the public-by-default processing resulted in a financial benefit to FB-I. I have outlined above how the public-by-default setting appears to be a deliberate choice on the part of FB-I, intended to maximise user engagement and sharing on the Instagram platform. While the lack of information in a clear and transparent form regarding this processing was not intentional, it nonetheless inhibited child users of Instagram from choosing to make their accounts private. Hence,

³⁹³ Ibid, paragraph 40

a proportion of those children are likely to have kept their profiles public, who otherwise may have opted for private profiles if FB-I had provided them the information on the purpose of the processing in a clear and transparent form. Public Instagram accounts prompt wider and more extensive sharing of user content, which in turn promotes user engagement with the service and advances the commercial interests of FB-I in terms of advertising sales. FB-I contends that this conclusion is speculative on the part of the DPC, and states that its business model *“primarily derives monetary income from targeted advertising, which - contrary to the Commission’s assertions - does not rely on users having public profiles”*. The DPC has not asserted that targeted advertising depends on a user having a public profile. Advertisements on Instagram are presented in the same “user feed” as user-generated content. Users are shown an aggregate of user-generated content and advertising content, which are formatted in a similar manner. The DPC’s view in this regard is that the public-by-default processing was intended to create user engagement on the platform by making users’ content more visible to other users, thereby increasing the overall amount of visible user-generated content on the platform for consumption, which in turn supports FB-I’s commercial objectives by providing user content which can be analysed, indexed and presented next to targeted advertising. This objective is clearly reflected in FB-I’s own submissions, where it states³⁹⁴:

*“Because sharing and maintaining an open exchange with the community of other users is at the heart of Instagram, setting profiles to public per default – including those of Teens – is appropriate and fully in line with user expectations. **Users expect to seek, discover, and connect with previously unknown content and communities on Instagram, and the user experience would be hampered for new users – who, by necessity, are still developing connections on Instagram – if their ability to participate would be restricted by default.** Default public settings are not only appropriate given the nature of the Instagram Service, which people join in order to use, but also because Facebook Ireland designed Instagram to be safe with Teens specifically in mind.”*
(emphasis added)

It is therefore clear that the public-by-default processing was designed to serve the purported “necessity” that child users would develop connections on Instagram. This was intended to create engagement between new users and other persons and content on the platform, by making new users’ content visible to others by default. While FB-I describes this processing as intended to serve the requirements of users, the objective of switching new accounts to “public” was clearly also intended to drive the creation of more public user-generated content for consumption, increasing engagement and creating favourable commercial conditions for the sale of targeted advertising by FB-I.

³⁹⁴ FB-I’s submission of 27 October 2020, Annex A, paragraphs 42 to 44

621. Therefore, I am satisfied that this infringement of Article 12(1) resulted in a financial benefit to FB-I. I consider that this is aggravating in the circumstances. For the purpose of this paragraph 621 (and paragraph 620, above), I have elaborated in more detail on the weight that I propose to give to this element in paragraph 624(5), below. For the avoidance of doubt, I am not aware of any relevant matters that fall to be considered, in the context of the contact information processing, for the purpose of this aspect of the assessment of the Article 6(1) infringement (and I note that FB-I has not sought, by way of the Final Submissions, to challenge this approach).

M.12 Decisions on whether to impose administrative fines

622. 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) cumulatively, as set out above. However, I have considered each distinct 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 proposed in ensuring compliance with the GDPR. The proposed order will assist in ensuring compliance by mandating specific action on the part of FB-I 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.

623. 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) for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 of the 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.”

624. While the order proposed 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 FB-I 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 FB-I and other controllers or processors carrying out similar processing operations concerning children’s data. 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. The infringement of Article 6(1) has been classed as falling at the upper end of the scale, in terms of seriousness, for the purpose of Article 83(2)(a). Both infringements of Article 12(1) and the single infringement of Article 5(1)(a) illustrate how non-compliance with transparency requirements can significantly increase the risk of serious harm to the rights and freedoms of data subjects and can prevent data subjects from mitigating such risks. I consider that this non-compliance must be strongly dissuaded and that administrative fines are necessary in order to effectively do so in this instance. Regarding the infringements of Articles 35(1), 24(1) and 25(1), in circumstances where FB-I processes a significant quantity of child users’ sensitive personal data, I consider that non-compliance with its obligations under these articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, I consider that administrative fines are appropriate and necessary in the circumstances. Finally, regarding FB-I’s infringements of Article 5(1)(c) and 25(2), processing children’s 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 because children are more likely to face obstacles in independently enforcing their own data protection rights. I have also had regard to how these infringements concerning the HTML source code processing subjected the personal data to potential web scraping. In those circumstances, I consider that administrative fines are appropriate and necessary in order to dissuade non-compliance.
- (2) 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 FB-I's infringements of Article 12(1) and 5(1)(c) and 25(2) regarding the public-by-default processing affected [REDACTED] data subjects. The loss of control suffered by the data subjects as a result of FB-I's infringements of Articles 6(1), 12(1), 5(1)(a), 5(1)(c) and 25(2) regarding the contact information processing affected a smaller, yet significant number of data subjects (I note that there are currently [REDACTED] child users with business accounts on Instagram in the European Region). All of the affected data subjects were children and I consider that the loss of control over personal data constitutes significant damage in the circumstances. In light of this damage, and how it was suffered by a significant number of children, I consider that fines are proportionate to responding to FB-I's particular infringements of Articles 6(1), 12(1), 5(1)(a), 5(1)(c) and 25(2) with a view to ensuring future compliance. I have also had regard to the financial benefit derived by FB-I as a result of the infringement of Article 12(1) regarding the public-by-default processing. I consider that this financial benefit also goes to the proportionality of the decision to impose an administrative fine. Finally, regarding FB-I's infringements of Articles 35(1), 24(1) and 25(1), I consider that administrative fines are proportionate in the circumstances because conducting DPIAs and implementing appropriate measures may require significant resources from controllers depending on the particular circumstances of the processing under consideration. It is proportionate to impose administrative fines to ensure compliance in light of how resource-based incentives for non-compliance may exist. In light of each of these factors, I consider that fines do not exceed what is necessary to enforce compliance in respect of each of the infringements identified in this Decision.

- (3) Each of the infringements carried either an intentional or negligent character. The intentional nature of FB-I's infringements of Articles 5(1)(a), 35(1), 5(1)(c) and 25(2) is aggravating when considering whether to impose administrative fines, and if so, the amount of those fines. FB-I intentionally omitted to carry out DPIAs, intentionally omitted to directly notify business account users of the change in the contact information processing, and intentionally processed personal data that was not limited to what was necessary for the purposes of the processing. The intentional nature of these infringements suggest that administrative fines are necessary to effectively ensure that FB-I makes decisions that comply with the GDPR in the future. I also consider that the negligent character of each of FB-I's infringements of Article 6(1), 12(1), 24(1) and 25(1) is also aggravating when considering whether to impose administrative fines, and if so, the amount of those fines. This negligence suggests that administrative fines are necessary to effectively ensure that FB-I directs sufficient attention to its obligations under Articles 6(1), 12(1), 24(1), and 25(1) in the future.

- (4) The categories of personal data affected by all of the infringements is also a factor that weighs heavily in favour of imposing administrative fines in respect of each infringement (including the infringement of Article 6(1) that was established by the EDPB in the Article 65 Decision). Each of the infringements relate specifically to children's personal data. Recital 38 of the GDPR recognises that children merit specific protection with regard to their personal data. This is a factor that I must have regard to when determining which corrective powers are appropriate, necessary and proportionate. I consider that administrative fines would help to ensure that FB-I and other similar controllers take the necessary action to ensure the upmost care is taken to avoid infringements of the GDPR in respect of children's data. In these particular circumstances where the categories of children's data affected by each of FB-I's infringements includes sensitive personal data in particular, due to the risk of contact from dangerous individuals, I consider that administrative fines are appropriate to provide specific protection to children's data.
- (5) In respect of FB-I's infringement of Article 12(1) regarding the public-by-default processing, I consider that the financial benefit accrued by FB-I as a result of this infringement merits an administrative fine in the circumstances. In circumstances where a controller or processor financially benefitted from infringing the GDPR, I consider that administrative fines are likely to be an appropriate corrective power to impose because an administrative fine acts to counter any financial incentives that may exist for controllers and processors who may infringe the GDPR either intentionally or negligently. While I am satisfied that, as set out in paragraph 620, above, it is appropriate for me to take account, as an aggravating factor, of the financial benefit accrued by FB-I as a result of this infringement, it is not possible for me to quantify the financial benefit gained, in the absence of evidence to support such an exercise. I note, in this regard, that, despite specific requests made by the DPC during the course of the Article 65 deliberations, no guidance has been provided by the EDPB, in its Article 65 Decision, as to the manner in which I might seek to calculate the value of the financial benefit gained on an objectively justifiable basis. In this regard, I note the views previously expressed by the EDPB³⁹⁵ that:

"... when deciding on the imposition of corrective measures in general, and fines in particular, "supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified"."

In terms, therefore, of the weight that might be attributed to this aspect of matters, I propose to take this factor into account as an aggravating factor of the

³⁹⁵ 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 28 July 2021, paragraph 403.

lightest possible weight. I consider that this weighting takes appropriate account of my view that a financial benefit was accrued by FB-I, as a result of the infringement, while having regard to the limitations on my ability to specifically quantify the value of the benefit gained.

(6) I have had regard to the lack of previous relevant infringements by FB-I, which is a slightly mitigating factor. I have also had regard to the actions taken by FB-I in order to remedy the infringement (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 proposed administrative fines (including the fine corresponding to the infringement of Article 6(1) GDPR). 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 children's personal data far outweighs the mitigation applied for this factor. Furthermore, despite the actions taken to remedy the infringements, and that mitigate the damage suffered as a result of the infringements, in light of the intentional and negligent character of all of the infringements, and FB-I's failure to comply with its obligations with regard to transparency, risk assessment, and data protection by design and default, I consider that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

(7) I have also taken account, as a slightly mitigating factor, of the fact that, for the purpose of Article 83(2)(i), corrective powers have not previously been ordered against FB-I with regard to the subject matter of this Decision. In circumstances, however, where the principle of accountability obliges controllers to be responsible for the implementation of the GDPR and where the GDPR has only been applicable since 25 May 2018, I am unable to attribute anything more than the lightest weight to this particular mitigating factor.

625. Regarding the infringements of Article 24(1), this article is not among the provisions captured by Article 83. Article 83(1) GDPR refers to the power of supervisory authorities to impose administrative fines *"in respect of infringements of [the GDPR] referred to in paragraphs 4, 5 and 6"*. While I have included findings in relation to FB-I's infringements of Article 24(1) GDPR, that provision is not referred to in Article 83(4), (5) or (6) GDPR. Therefore, it is not possible to impose an administrative fine in respect of the infringements of Article 24(1) GDPR. Further to this, my consideration of Article 24 above is separate to my consideration of other infringements, and I have not considered the Article 24 infringement to be an aggravating factor in respect of the other infringements.

626. Based on the analysis I have set out above, I propose to impose the following administrative fines:

- (1) In respect of FB-I's infringement of Article 12(1) regarding the public-by-default processing (**Finding 1**), I proposed a fine of between €55 million and €100 million.
- (2) In respect of FB-I's infringement of Article 12(1) regarding the contact information processing (**Finding 2**), I proposed a fine of between €46 million and €75 million.
- (3) In respect of FB-I's infringement Article 5(1)(a) regarding the contact information processing (**Finding 4**), I proposed a fine of between €9 million and €28 million.
- (4) In respect of FB-I's infringement of Article 35(1) regarding the contact information processing (**Finding 5**), I proposed a fine of between €28 million and €45 million.
- (5) In respect of FB-I's infringement of Article 35(1) regarding the public-by-default processing (**Finding 6**), I proposed a fine of between €28 million and €45 million.
- (6) In respect of FB-I's infringement of Articles 5(1)(c) and 25(2) regarding the contact information processing (**Finding 7**), I proposed a fine of between €9 million and €28 million.
- (7) In respect of FB-I's infringement of Articles 25(1) regarding the contact information processing (**Finding 8**), I proposed a fine of between €9 million and €28 million.
- (8) In respect of FB-I's infringement of Articles 5(1)(c) and 25(2) regarding the public-by-default processing (**Finding 10**), I proposed a fine of between €9 million and €28 million.
- (9) In respect of FB-I's infringement of Article 25(1) regarding the public-by-default processing (**Finding 11**), I proposed a fine of between €9 million and €28 million.
- (10) In respect of FB-I's infringement of Article 6(1) regarding the contact information processing (**Finding 13**), I proposed a fine of between €9 million and €28 million.

627. In having determined the quantum of the fines proposed 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. 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 sensitive personal data belonging to children and the infringements all increased the risks posed by the processing to the right and freedoms of those children.

628. 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.

629. As regards the requirement for any fine to be “*proportionate*”, this requires me to adjust the quantum of any proposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fines proposed above do not exceed what is necessary to enforce compliance with the GDPR taking into account the size of FB-I’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.

630. In its response to the PDD³⁹⁶, FB-I contends that the fines proposed are unprecedented, and should not be applied in respect of transparency standards which were not previously articulated to FB-I. In this regard, I note that the GDPR does not depend on ancillary guidance documents for its legal application; FB-I was obliged to comply with Article 12 since May 2018, without the need for additional legislative guidance. It is an inherent feature of the GDPR that its provisions are not prescriptive; FB-I was obliged to assess the quality of its transparency measures in light of the specific processing at issue, and in order to respect the principle of accountability. FB-I further contends that it would be disproportionate to propose high fines for an infringement of Article 12, if the information in question was otherwise provided in compliance with Article 13. I do not agree with FB-I in this regard. Article 12(1) is not a subsidiary legal provision, and constitutes a legal obligation in its own right. This is especially true in the present circumstances, which involve the provision of information to children on processing (bearing in mind that Article 12(1) specifically requires that information provided to children in particular must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language). I also note that Article 12 is expressly included among the infringements which attract higher possible fines under Article 83(5) GDPR. I am therefore of the view that the provision of Article 13 information, in an inadequate form from the perspective of child users, would not cure or mitigate the Article 12(1) infringement. FB-I also reiterates its opposition to the substance of the transparency findings, and in particular states that it ought to be allowed a margin of flexibility in how it arranges its transparency measures, and contends that the DPC has taken a prescriptive approach to transparency measures. I do not agree with FB-I’s summary of my findings, for reasons which are set out in full at Part F of this Decision.

631. Finally, FB-I contends³⁹⁷ that the proposed fines are disproportionate by reference to fines levied in two other GDPR decisions of EU supervisory authorities. Direct comparison of the amount of fines in different cases is a limited way to assess the proportionality of

³⁹⁶ FB-I’s submission of 9 August 2021, paragraphs 132 to 135

³⁹⁷ Ibid, paragraph 135

the proposed fines in the present case, because each case turns on its unique factual circumstances. The calculation of a fine takes into account many factual considerations which will not be evident from a surface level assessment of the eventual fine. I also note that Articles 58(2)(i) and 83(2) each expressly state that administrative fines depend on the circumstances of the individual case. While the decisions cited by FB-I relate generally to transparency obligations, I am satisfied that the specific factual circumstances of this individual case, as described in detail above, require the application of the proposed fine in order to ensure the fines are effective, proportionate and dissuasive.

632. FB-I also contends³⁹⁸ that the proposed fine should be reduced on the basis that it is “arbitrary, excessive, and disproportionate”. FB-I submits that the need for a dissuasive fine is reduced in circumstances where FB-I has otherwise made relevant service changes since the time of the infringements. I do not agree with FB-I in this regard. Instagram is a constantly evolving service which involves the processing of personal data of millions of children. Without prejudice to the GDPR compliance of recent service changes made by FB-I, the need for a dissuasive fine is also evident in order to inform FB-I’s future service developments and innovations (in terms of transparency and risk assessment). The proposed fines also serve to dissuade similar non-compliance by other controllers; the service changes made by FB-I do not modify the need to dissuade other controllers from similar infringements of the GDPR.

633. In relation to the infringement of Article 6(1) that was established by the EDPB in the Article 65 Decision, I consider the fining range set out above to be effective, proportionate and dissuasive, taking into account:

- a. The purpose of the fine, which is to sanction the infringement of Article 6(1) GDPR that was found to have occurred (by the EDPB in the Article 65 Decision) and to re-establish compliance with the GDPR;
- b. The requirement for any fine to not exceed what is necessary to achieve the stated objective (as recorded at a., above). In this regard, the DPC has taken account of the views expressed by the EDPB at paragraph 235 of the Article 65 Decision. For the avoidance of doubt, the DPC has also reflected upon the totality of fines proposed in this case. The DPC considers that, taken as a whole, the fines proposed are proportionate to the circumstances of the case, taking into account the matters identified by the EDPB at paragraph 235 of the Article 65 Decision;
- c. The circumstances of the case, by reference to the assessments and conclusions of the EDPB, as set out in paragraphs 80 to 100 (inclusive) and 101 to 132 (inclusive) of the Article 65 Decision together with the criteria of

³⁹⁸ FB-I’s submission of 9 August 2021, paragraph 155

particular significance identified in paragraph 134 of the Article 65 Decision. I have taken particular account, in this regard, of the facts that:

- i. In relation to the EDPB's assessment that resulted in the finding that FB-I was not entitled to rely on Article 6(1)(b) when processing the contact information of child users, the EDPB recognised the existence of a two limb test³⁹⁹ comprising, firstly, the requirement for the processing to take place in the context of the performance of a contract with the data subject and, secondly, for the processing to be necessary for the performance of that particular contract with the data subject. As regards the first limb of the test, the Article 65 Decision does not record any definitive finding of non-compliance by FB-I in this regard. It was by reference to the second limb of the test that the EDPB concluded that FB-I was not entitled to process the contact information of child users in reliance on Article 6(1)(b) GDPR. As regards that particular finding, however, the DPC recalls that the EDPB's conclusion was partially based on the impact of FB-I's lack of transparency as well as the DPC's own assessment, as regards FB-I's infringement of Article 5(1)(c). Both of these matters are the subject of separate fines and the DPC has taken this into account when proposing the fining range set out above so as to avoid the risk of punishing FB-I twice in respect of the same conduct.
- ii. In relation to the EDPB's assessment that resulted in the finding that FB-I was not entitled to rely on Article 6(1)(f) when processing the contact information of child users, the EDPB recognised the existence of a three limb test⁴⁰⁰ comprising, firstly, the requirement for the existence of a legitimate interest, secondly, the requirement for a need to process the personal data for the purposes of the legitimate interest pursued and, thirdly, that the fundamental rights and freedoms of the data subject do not take precedence. As regards the first and second limbs of the test, the Article 65 Decision does not record any definitive findings of non-compliance by FB-I, in this regard. It was by reference to the third limb of the test that the EDPB concluded that FB-I was not entitled to process the contact information of child users in reliance on Article 6(1)(f) GDPR. As regards that particular finding, however, the DPC recalls that the EDPB's conclusion was partially based on the impact of FB-I's lack of transparency. This matter, however, is the subject of a separate fine

³⁹⁹ The Article 65 Decision, paragraph 80

⁴⁰⁰ The Article 65 Decision, paragraph 103

and the DPC has taken this into account when proposing the fining range set out above so as to avoid the risk of punishing FB-I twice in respect of the same conduct.

- d. The requirement for a genuinely deterrent effect, in terms of discouraging both FB-I and others from committing the same infringement in the future; and
- e. The requirement for any fine to reflect the gravity of the infringement, taking into account all the elements that may lead to an increase (aggravating factors) or decrease (mitigating factors) of the initial assessment.

634. By way of the Final Submissions⁴⁰¹, FB-I disagreed with the above, by reference to:

- a. Its submissions concerning the nature and consequences of the infringement (which I have already taken into account within the Article 83(2) assessment, above);
- b. The fact that there was disagreement amongst the CSAs over the application of Articles 6(1)(b) and (f) and that, while this disagreement was ultimately resolved by the EDPB, the Article 65 Decision is not definitive in respect of a number of important limbs of the relevant tests to be applied. I have already addressed the first part of FB-I's submission within the Article 83(2) assessment, above. As regards the second aspect, I have already taken this into account when assessing the fining range that should be applied to the Article 6(1) infringement;
- c. The "near complete, if not total, overlap between the activities the subject of fines for infringements of Articles 5 and 12 GDPR and Article 6 GDPR". I note that I have already taken this factor into account when assessing the applicable fining range;
- d. The fact that the infringements already found in respect of Articles 5, 12 and 25 GDPR are already subject to very significant fines. In these circumstances, an additional fine in the range proposed is not necessary to have a deterrent effect or to discourage FB-I or others from committing the same infringements in the future. I disagree with this aspect of FB-I's submissions. I am of the view that the application of a lower fining range would have the effect of giving the impression to both FB-I and other data controllers that infringements of Article 6 are somehow less serious than the other infringements that were found to have occurred.

⁴⁰¹ The Final Submissions, paragraphs 32 to 35 (inclusive)

635. Having considered FB-I's submissions, I am satisfied that the ten fines specified at paragraph 626 would, if imposed on FB-I, be effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

M.13 Article 83(3)

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

637. 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."

638. In the PDD, I considered that FB-I's infringement of Article 12(1) was the gravest infringement concerning the public-by-default processing, and similarly, that FB-I's infringement of Article 12(1) is the gravest infringement concerning the contact information processing.

639. Subsequent to the finalisation of the PDD, the EDPB adopted a binding decision ("**the EDPB Decision concerning WhatsApp**")⁴⁰² 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.

640. The EDPB Decision concerning WhatsApp applies an interpretation of Article 83(3) GDPR that differs from the interpretation I set out in the PDD. 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 future inquiries given that it is a matter of general interpretation that is not specific to the facts of the case in which it arose.

641. 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

⁴⁰² https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.

316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.

317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.

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

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

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

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

finer highly contributes to enforcement and therefore to compliance with the GDPR.

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

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

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

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

duty on the SA imposing the fine to take into account the proportionality of the fine.

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

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

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

643. As stated previously, I consider that FB-I’s infringement of Article 12(1) is the gravest infringement concerning the public-by-default processing, and similarly, that FB-I’s infringement of Article 12(1) is the gravest infringement concerning the contact information processing. I further note that the associated maximum possible fine for these infringements under Article 83(5) GDPR is 4% of the turnover of Meta Platforms, Inc., formerly Facebook 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 proposed ranges for the individual infringements are added together, a fining range of between €211 million to €433 million arises. The proposed fine is below 4% of the turnover of Meta Platforms, Inc. as considered below.

644. FB-I has already provided submissions on the PDD, which clearly set out its view on the approach to fines in this matter (without prejudice to FB-I’s view that no infringement of the GDPR has taken place). As the EDPB Decision concerning WhatsApp was adopted

subsequent to FB-I having made submissions on the PDD, I afforded FB-I an additional opportunity to make submissions on this specific matter: that is, the EDPB's interpretation of Article 83(3) GDPR. The purpose of the additional opportunity for submissions was to address the interpretation of Article 83(3) GDPR in the EDPB Decision and its application to this Inquiry, not to reopen the question of the appropriate quantum for any administrative fine and/or to provide for an additional round of submissions on that issue. In my letter of 25 November 2021, I also noted that FB-I had recently made submissions on the interpretation of Article 83(3) GDPR in the context of the separate Inquiry IN-18-5-5; accordingly, I asked FB-I if it wished to sustain similar objections in the present Inquiry, while also inviting FB-I to address any other pertinent matters in its response. FB-I subsequently responded to the DPC on 2 December 2021.

645. As a preliminary matter, FB-I has objected to the manner in which it has been asked to make submissions on Article 83(3). In particular, FB-I states that it was not provided with the revised Draft Decision, or relevant extracts of the revised PDD relating to the DPC's interpretation of Article 83(3), before making its submission on Article 83(3) GDPR. This, in its view, results in a requirement to make submissions "in the abstract".

646. As is set out in this Decision, FB-I has already been afforded an opportunity to make comprehensive submissions on the PDD that addressed every factor proposed by the DPC for consideration in determining, if any, the appropriate fine. It was not the intention of the DPC, in this regard, to seek additional submissions from FB-I on the reasoning for a particular fining range, those submissions having already been made in detail. The purpose of requesting new submissions, on this point, was to enable FB-I to exercise its right to be heard on the application of the interpretation of Article 83(3) GDPR in the EDPB Decision. In this regard, FB-I has stated that its detailed submission of 23 September 2021 on Article 83(3) GDPR applies to the present circumstances. On this basis, I do not accept that FB-I has been deprived of the opportunity to meaningfully exercise its right to be heard.

647. FB-I's response of 2 December 2021 also states that the DPC should not "adopt a uniform approach to the application of Article 83(3) GDPR in all inquiries". I am satisfied in this regard that I have had due regard in this Inquiry to the individual circumstances which bear on the application of Article 83(3) GDPR. I also note in this regard that although FB-I was invited to address any relevant matters in its response, it has not raised any specific legal or factual points which pertain uniquely to the application of Article 83(3) in this Inquiry. I also note that while the application of Article 83(3) GDPR turns on the factual circumstances of each individual case, certain interpretative approaches are common to all applications of the law.

648. In its response of 2 December 2021, FB-I confirmed that its objections⁴⁰³ raised in Inquiry IN-18-5-5 concerning the DPC's interpretation of Article 83(3) GDPR were "*equally applicable to the reasoning underlying any Revised PDD in this Inquiry*". I have therefore considered FB-I's submission of 23 September 2021 in the context of this inquiry.

649. In its submission of 23 September 2021, FB-I has argued that the above interpretation and application of Article 83(3) GDPR is incorrect and/or should not be applied because: the EDPB decision is incorrect as a matter of law and is, in any event, not binding on the DPC; even if the decision were binding on the DPC, it does not require that the DPC impose administrative fines in the manner proposed; the DPC has not had regard to the criteria of effectiveness, proportionality and dissuasiveness in Article 83(1) GDPR when determining the total cumulative proposed fine; and no decision on the correct interpretation of Article 83(3) GDPR should be made prior to the determination of certain proceedings⁴⁰⁴ before the General Court of the Court of Justice of the European Union to annul the EDPB Decision concerning WhatsApp ("the **Annulment Proceedings**").

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

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

652. It is not the position of the DPC that the EDPB in and of itself has the power to issue decisions of general application that bind supervisory authorities. The issue is not the powers or functions of the EDPB, but rather the legal responsibility of the DPC to the concerned supervisory authorities, who in themselves happen to be constituent members of the EDPB. In this regard, assistance is provided in the interpretation of the

⁴⁰³ FB-I's submission of 23 September 2021

⁴⁰⁴ WhatsApp Ireland v Comité européen de la protection des données, Case T-709/21

DPC's duties under Article 60(1) GDPR by Recital 123, which states that "*...supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union...*". The DPC's view is that the duty to cooperate and ensure consistency that is placed on it by the GDPR would be rendered ineffective were it not to ensure, to the best of its ability, such interpretations were applied consistently.

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

654. FB-I has argued that the EDPB Decision "*did not direct the [DPC] to impose separate fines in respect of each infringement and to then add those fines together*", but rather that the final amount should be considered in accordance with the requirements that the fine be effective, proportionate and dissuasive pursuant to Article 83(1) GDPR. It submits further submits that the fine would be contrary to the EU law principles of proportionality, *ne bis in idem* and concurrence of laws.

655. FB-I develops this aspect of its argument in a later section of its submission, by suggesting that "*it appears...that the [DPC] does not propose to engage in any meaningful assessment of whether the total fine [meets the Article 83(1) GDPR criteria]*". FB-I contends (both in its response of 2 December 2021, and the submission of 23 September 2021) that because the DPC viewed the fine proposed in the PDD as effective, proportionate and dissuasive, a higher fine must be regarded as going beyond that standard. FB-I also argues that its ability to make submissions in relation to this new proposed fine is "restricted" due to it not being given sight of the entire working draft, or relevant extracts of the revised PDD.

656. In relation to the requirements of Article 83(1) GDPR, which includes the EU law principle of proportionality relied on by FB-I, the DPC refutes any suggestion that it has not had regard to this provision in proposing a final fine. Part M.12 of this Decision sets out, in detail, the DPC's reasoning as to why the proposed fine is effective, proportionate, and dissuasive. Moreover, as has been set out, FB-I has provided extensive submissions on the PDD as to its views on what an effective, dissuasive and proportionate sanction would be. I therefore reject any suggestion that there was "*a failure to adequately consider whether, taken as a whole, the proposed fines in respect of all the infringements are effective, proportionate and dissuasive*".

657. FB-I has already provided extensive submissions on the PDD, which clearly set out its view on the approach to fines in this matter, without prejudice to its view that no infringement of the GDPR has taken place. The purpose of the additional opportunity for submissions referred to here was to address the interpretation of Article 83(3) GDPR in the EDPB Decision and its application to this Inquiry, not to reopen the question of the appropriate quantum for any administrative fine and/or to provide for an additional round of submissions on that issue. The DPC in any event rejects any suggestion that the Article 83(1) GDPR criteria are not met by the new fine on the application of the new interpretation of Article 83(3) GDPR, and as is seen in Part M.12 above, I have given due consideration to this and to FB-I's submissions in this regard. I therefore remain satisfied that the proposed application of Article 83(3) GDPR is consistent with Article 83(1) GDPR, for the reasons set out here and in Part M.12.

658. In relation to the alleged contravention of the *ne bis in idem* principle (to the extent that FB-I contends that it applies to the present circumstances) I also reiterate the views expressed in Part M herein, which sets out that the infringements at issue each constitute distinct breaches of different GDPR obligations. The legislator has provided for distinct requirements, and each individual requirement identified above has been infringed by FB-I. For these reasons and the reasons set out above, I do not accept this submission in the present circumstances. Similarly, the DPC is not applying a new and retroactive view of wrongdoing to the conduct in a manner envisaged by principle of concurrence of laws. It is simply determining the proper interpretation of Article 83(3) GDPR. This has no impact on the DPC's detailed consideration of FB-I's submissions on the separate and more general question of the appropriate penalty.

659. It also argues that the taking into account of the undertaking's turnover is incorrect as a matter of law, as it is not set out as a factor in Article 83(2) GDPR. In this regard, the DPC relies on its existing analysis of its obligations to cooperate with the concerned supervisory authorities and apply the GDPR consistently. For the same reasons provided to support the DPC's decision to apply the interpretation of Article 83(3), as in the EDPB Decision concerning WhatsApp, in general, the DPC intends to maintain this consideration of the undertaking's turnover.

660. Finally, FB-I has argued that, in light of the intended Annulment Proceedings in respect of the EDPB Decision concerning WhatsApp, the DPC should not finalise this Decision until a final decision as to the correct interpretation of Article 83(3) GDPR has been made by the CJEU. FB-I's submission is simply that "*there is, at a minimum, very considerable doubt as to the correct interpretation of Article 83(3) GDPR*" and that on this basis the DPC should not proceed with this Decision until the matter is finalised. FB-I has provided no legal authority in support of this proposition. Notwithstanding the possible overlap between some of the questions referred and the issues arising for decision in this Inquiry, given the advanced stage of this Inquiry I am satisfied that there is no reason to delay

this matter. The prospect of intended legal proceedings in respect of a separate decision does not provide any basis in law for suspending a separate Inquiry.

M.13 Articles 83(4) and (5) GDPR

661. Turning, finally, to Articles 83(4) and (5) GDPR, I note that these provision operate to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

662. Article 83(4) 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;

663. Article 83(5) provides as follows:

“Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects’ rights pursuant to Articles 12 to 22;

...”

664. 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.”

665. 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 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”⁴⁰⁵.

666. 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 infringement⁴⁰⁶.

667. 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.

668. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case⁴⁰⁷.

669. The CJEU has, however, established⁴⁰⁸ 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.

⁴⁰⁵ Höfner and Elser v Macrotron GmbH (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161, paragraph 21.

⁴⁰⁶ Akzo Nobel and Others v Commission, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, paragraphs 58 – 60.

⁴⁰⁷ Ori Martin and SLM v Commission (C-490/15 P, judgment delivered 14 September 2016) ECLI:EU:C:2016:678, paragraph 60.

⁴⁰⁸ Akzo Nobel and Others v Commission, (C-97/08 P, judgment delivered 10 September 2009).

670. 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 subsidiary⁴⁰⁹.

671. 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 subsidiary⁴¹⁰. 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 ...”*⁴¹¹

672. 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.

673. It is important to note that “*decisive influence*”, in this context, refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR, in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.

674. As noted above, within the European Region, the Instagram service is provided by a subsidiary of Meta Platforms, Inc. known as Facebook Ireland Limited (referred to as “FB-

⁴⁰⁹ Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, paragraph 48.

⁴¹⁰ Judgments of 7 June 2011, *Total and Elf Aquitaine v Commission*, T-206/06, not published, EU:T:2011:250, paragraph 56; of 12 December 2014, *Repsol Lubricantes y Especialidades and Others v Commission*, T-562/08, not published, EU:T:2014:1078, paragraph 42; and of 15 July 2015, *Socitrel and Companhia Previdente v Commission*, T-413/10 and T-414/10, EU:T:2015:500, paragraph 204.

⁴¹¹ Opinion of Advocate General Kokott in *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:262, point 73 (as cited in judgment of 12 July 2018, *The Goldman Sachs Group, Inc. v European Commission*, Case T-419/14, ECLI:EU:T:2018:445, paragraph 51).

I” in this Decision). FB-I’s ultimate parent is Meta Platforms, Inc. I have had regard to FB-I’s Director’s Report and Financial Statements for the Financial Year ended 31 December 2019, which are available from the Companies Registration Office and are dated December 2020. 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.”

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

“At 31 December 2019, the company is a wholly-owned subsidiary of Facebook International Operations Limited, a company incorporated in the Republic of Ireland, its registered office being 4 Grand Canal Square, Grand Canal Harbour, Dublin 2.

The ultimate holding company and ultimate controlling party is Facebook, Inc., a company incorporated in Wilmington, Delaware, United States of America. The ultimate holding company and controlling party of the smallest and largest group of which the company is a member, and for which consolidated financial statements are drawn up, is Facebook, Inc.”

676. For the purpose of the PDD, I assumed that the above has remained the position in the interim. I note, in this connection, that the same position was stated in FB-I’s Directors’ Report and Financial Statements for the year ended 31 December 2018, which is dated November 2019. I also note in relation to the above that Facebook, Inc. changed its name to Meta Platforms, Inc. as of 28 October 2021.

677. On this basis, it is my understanding that FB-I 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 FB-I 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 [FB-I] is a member ... is Facebook, Inc. [now known as Meta Platforms, Inc.]”*. It is therefore assumed that Meta Platforms, Inc. is in a similar situation to that of a sole owner as regards its power to (directly or indirectly) exercise a decisive influence over the conduct of FB-I.

678. It seemed therefore at the time of preparing the PDD, that the corporate structure of the entities concerned is such that Meta Platforms, Inc. is in a position to exercise decisive influence over FB-I’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 FB-I on the market.

679. If this presumption is not rebutted, it would mean that Meta Platforms, Inc. and FB-I 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 Articles 83(4) and (5) GDPR, would fall to be determined by reference to the combined turnover of FB-I and Meta Platforms, Inc.

680. In its response to the PDD, FB-I has made submissions⁴¹² in this regard in an attempt to rebut the presumption of decisive influence. In particular, FB-I submitted that the presumption of decisive influence on the market does not translate into a data protection context without considering what “behaviour on the market” means in a data protection context. It argues that this analysis should focus instead on the entity that has the decision-making capacity in the context of data protection matters, rather than matters relating to the market in general as is the case in competition law. I do not agree with this assessment. Firstly, the suggested approach (involving an assessment of where the decision-making power lies, in relation to the processing of personal data) is effectively a replication of the assessment that must be undertaken at the outset of the Inquiry process, the outcome of which determines (i) the party/parties to which the Inquiry should be addressed; and (ii) (in cross border processing cases) the supervisory authority with jurisdiction to conduct the Inquiry. Given the consequences that flow from this type of assessment, it would not be appropriate for this assessment to be conducted at the decision-making stage of an Inquiry.

681. Secondly, the suggested approach could not be applied equally in each and every case. Where, for example, the presumption of decisive influence has been raised in the context of a cross-border processing case where one of the entities under assessment is outside of the EU, an assessment of that entity’s ability to exercise decisive influence over the respondent’s data processing activities would likely exceed the scope of Article 3 GDPR. Such a scenario risks undermining the DPC’s ability to comply with its obligation, pursuant to Article 83(1) GDPR, to ensure that the imposition of fines, in each individual case, is “effective, proportionate and dissuasive”.

682. Finally “behaviour on the market” has a meaning normally ascribed to it in EU competition law. In summary, “behaviour on the market” describes how an entity behaves and conducts its affairs in the context of the economic activity in which it engages. Such behaviour will include matters such as the policies and procedures it implements, the marketing strategy it pursues, the terms and conditions attaching to any products or services it delivers, its pricing structures, etc. I therefore can see no basis in

⁴¹² FB-I’ submission of 9 August 2021, paragraph 156

law, in FB-I's submissions or otherwise, to deviate from this well-established principle as set out both in the GDPR, other provisions of EU law and the jurisprudence of the CJEU.

683. In the PDD and Draft Decision, I calculated the administrative fine on the basis that Facebook, Inc. (as it was then called) had a reported a total revenue of \$85.965 billion U.S. dollars for the year ended 31 December 2020⁴¹³. As I noted in that Draft Decision, FB-I contended that the term "preceding financial year" in Article 83(5) GDPR should be construed as a reference to the financial year that precedes the infringements, or the year preceding the commencement of the Inquiry.⁴¹⁴ I noted that it was FB-I's position that the term "preceding financial year" should not be construed as a reference to the year preceding the imposition of a fine.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

684. In considering the relevant year for the turnover for the purposes of Article 83(5), the Board stated that it *"agrees with the approach taken by the IE SA for the present case to include in the Draft Decision a provisional turnover figure based on the most up to date financial information available at the time of circulation to the CSAs pursuant to Article 60(3) GDPR. The EDPB recalls that when issuing its final decision in accordance with Article 65(6) GDPR, the IE SA shall take into account the undertaking's annual turnover corresponding to the financial year preceding the date of its final decision, i.e. the turnover of Meta Platforms Inc. in 2021."*⁴¹⁵

685. On the basis of the above, I am satisfied that I am required to have regard to Facebook, Inc.'s (now Meta Platform, Inc.) turnover for the year ended 2021. FB-I have confirmed that *"the combined turnover for the Meta Platforms, Inc. group of companies for the year ending 31 December 2021 was approximately \$117.929 billion."*⁴¹⁶

686. Applying the above to Articles 83(4) and (5) GDPR, I first note that, in circumstances where the fine is being imposed on an "undertaking", a fine of up to 4% (in respect of the infringements of Articles 5(1)(a), 5(1)(c) and 12(1) GDPR), and a fine of up to 2% (in respect of infringements of Article 25(1) Article 25(2), and Article 35 GDPR) of the undertaking's total worldwide annual turnover of the preceding financial year may be imposed. I further note that the proposed fines are (respectively) less than 4% and 2% of Meta Platforms, Inc.'s total worldwide annual turnover for the year 2020. That being the

⁴¹³ Press Release, 'Facebook Reports Fourth Quarter and Full Year 2020 Results' available at <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/>.

⁴¹⁴ FB-I' submissions of 9 August 2021.

⁴¹⁵ EDPB's Binding Decision 02/2022, at para/ 194.

⁴¹⁶ Letter dated 28 July 2022 from FB-I to the DPC, referencing financial information which is available at: <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>

case, the fines proposed above do not exceed the applicable fining “caps” prescribed by Articles 83(4) and (5) GDPR.

N. Summary of Envisaged Action

687. In summary, the corrective powers that I propose to exercise are:

688. An order pursuant to Article 58(2)(d) to FB-I to bring its processing into compliance with the GDPR in the manner specified in this Decision. It is proposed that this should be done within three months of the date of notification of any final decision;

689. A reprimand to FB-I pursuant to Article 58(2)(b) of the GDPR regarding the infringements identified in this Decision ; and

690. Ten administrative fines, as follows:

1. In respect of FB-I’s infringement of Article 12(1) regarding the public-by-default processing (**Finding 1**), a fine of €100 million.
2. In respect of FB-I’s infringement of Article 12(1) regarding the contact information processing (**Finding 2**), a fine of €70 million.
3. In respect of FB-I’s infringement Article 5(1)(a) regarding the contact information processing (**Finding 4**), a fine of €25 million.
4. In respect of FB-I’s infringement of Article 35(1) regarding the contact information processing (**Finding 5**), a fine of €45 million.
5. In respect of FB-I’s infringement of Article 35(1) regarding the public-by-default processing (**Finding 6**), a fine of €45 million.
6. In respect of FB-I’s infringement of Articles 5(1)(c) and 25(2) regarding the contact information processing (**Finding 7**), a fine of €25 million.
7. In respect of FB-I’s infringement of Articles 25(1) regarding the contact information processing (**Finding 8**), a fine of €25 million.
8. In respect of FB-I’s infringement of Articles 5(1)(c) and 25(2) regarding the public-by-default processing (**Finding 10**), a fine of €25 million.
9. In respect of FB-I’s infringement of Article 25(1) regarding the public-by-default processing (**Finding 11**), a fine of €25 million.
10. In respect of FB-I’s infringement of Article 6(1) regarding the contact information processing (**Finding 13**), a fine of €20 million.

691. In having selected the specific figures, in respect of the infringements identified a numbers 1 to 10, above, from the upper end of the fining ranges that were proposed by way of the PDD, 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 the supervisory authorities, as expressed during the course of the Article 60(3) GDPR consultation period. In this regard, Article 60(3) requires the DPC to take “due account” of the views that might be expressed by the CSAs. That obligation applies regardless of whether the views have been expressed by way of a relevant and reasoned objection or otherwise;
- d. The views expressed by the EDPB, at paragraphs 235 and 236 of the Article 65 Decision and, in particular, the statement that “the EDPB considers that in the present case each fine should fall within the higher segment of the envisaged fine amount ranges, in order to be sufficiently effective and dissuasive in accordance with Article 83(2) GDPR.”
- e. The views expressed by FB-I in the various submissions furnished on fining matters, including the Final Submissions. I note, in this regard, that FB-I has submitted that the EDPB is not competent to direct the DPC on the quantum of any fine and neither is the DPC bound to follow the views set out at paragraphs 235 and 236 of the Article 65 Decision. I disagree with this suggestion. Even, however, if it were correct, it would not change the fact that, of those CSAs that expressed views on the quantum of the fining ranges that were proposed by the Draft Decision, all indicated a preference for the imposition of significant fines. As noted, above, the DPC is obliged, by Article 60(3) to take “due account” of such views. Otherwise, the manner in which I have taken account of the matters raised in Section II of FB-I’s Final Submissions is already addressed, under the relevant heading of the Article 83 assessment, above.

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

This Decision is addressed to:

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

Dated the 2nd day of September 2022

Decision-Maker for the Commission:

[sent electronically, without signature]

**Helen Dixon
Commissioner for Data Protection**

Appendix 1 – The Article 65 Decision