In the matter of the General Data Protection Regulation

DPC Inquiry Reference: IN-18-12-2

In the matter of WhatsApp Ireland Limited

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 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 20th day of August 2021

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Table of Contents

Introduction

1. This is the decision ("the **Decision**") of the Data Protection Commission ("the **Commission**"), made pursuant to Section 111 of the Data Protection Act, 2018 ("the **2018 Act**") and in accordance with Articles 60 and 65 of the General Data Protection Regulation ("the **GDPR**"). I have made this Decision as the Decision-Maker for the Commission, following an inquiry, conducted pursuant to Section 110 of the 2018 Act, concerning the question of compliance or otherwise by WhatsApp Ireland Limited ("**WhatsApp**") with its obligations pursuant to Articles 12, 13 and 14 of the GDPR. The purpose of this Decision is to record the Commission's views, as to whether or not an infringement of the GDPR has occurred/is occurring and the corrective powers that will be exercised, in response to any finding(s) of infringement. For the avoidance of doubt, the subject matter of this Decision was previously addressed by way of separate draft decisions, as follows:

    a. The Commission's understanding of the relevant factual background and its provisional views, as to whether or not one or more infringements of the GDPR has occurred/is occurring, were previously addressed by way of the Preliminary Draft Decision that issued to WhatsApp Ireland Limited on 21 May 2020 ("the **Preliminary Draft**"); and

    b. The Commission's provisional views, as to whether one or more corrective powers should be exercised in the event of any (concluded) finding that one or more infringements has occurred/is occurring, were previously addressed by way of the Supplemental Draft Decision that issued to WhatsApp on 20 August 2020 ("the **Supplemental Draft**").

2. This Decision represents the views of the Commission, for the purposes of Article 60 of the GDPR, on the matters that were previously separately addressed in the Preliminary Draft and Supplemental Draft decisions. It further reflects the binding decision made by the European Data Protection Board ("the **Board**" or, otherwise, "the **EDPB**") pursuant to Article 65(2) of the GDPR[1], which directed changes to certain of the positions in the draft decision that was presented by the Commission for the purposes of Article 60, as detailed further below ("the **Article 65 Decision**").

Basis of Inquiry

3. Following the entry into force of the GDPR on 25 May 2018, the Commission received a number of complaints from individual data subjects concerning the data processing activities of WhatsApp. These complaints were received from both users and non-users of WhatsApp's services. In addition to this, the Commission also received a mutual assistance request, pursuant to Article 61 of the GDPR, from Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (the German Federal Data Protection Authority). That request touched upon the transparency obligations that are placed on data controllers by the GDPR in the context of the possible sharing of personal data between WhatsApp and a variety of Facebook companies.

4. Following a preliminary examination of the complaints, the Commission observed that, while the precise details of the complaints differed, concerns about transparency featured as a common theme throughout. Having considered the issues arising, the Commission decided to commence an own-volition inquiry pursuant to Section 110 of the 2018 Act for the purpose of assessing the extent to

[1] 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

which WhatsApp complies with its transparency obligations pursuant to Articles 12, 13 and 14 of the GDPR.

5. It is important to note, at this juncture, that, while the decision to commence an own-volition inquiry was prompted by the common theme running across the various complaints and the above-referenced mutual assistance request, this inquiry is not an inquiry into any specific or individual complaint, concern or request. The Commission will (to the extent that it has not already done so) handle any such individual complaints or concerns by way of separate processes under the 2018 Act, as might be required. For the avoidance of doubt, neither the Investigator nor I, as Decision-Maker, have had regard to any individual complaint(s), concern(s) or request(s) for mutual assistance for the purpose of the within inquiry.

Competence of the Commission

6. Given that WhatsApp delivers services to individuals across Europe, it was necessary to consider the extent of the Commission's jurisdiction in the context of the within inquiry. In this regard, Article 56 of the GDPR provides that:

> *"… the supervisory authority of the main establishment or the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."*

<u>WhatsApp's position as to its establishment in Ireland</u>

7. WhatsApp previously notified the Commission, by way of email dated 25 May 2018 ("the **25 May Email**"), that:

> *"… WhatsApp Ireland Limited (acting as the data controller for the WhatsApp service in the EU) will have its main establishment in the European Union in Ireland."*

8. The Investigator, upon commencement of the within inquiry, requested that WhatsApp confirm whether the processing of personal data which is the subject matter of the inquiry satisfied the definition of "*cross-border processing*" set out in Article 4(23)(b) of the GDPR. She further requested confirmation that the position, as regards the identity and location of the main establishment, for the purpose of the WhatsApp service, remained as outlined in the 25 May Email.

9. WhatsApp confirmed the former and affirmed the latter as part of its response to the Investigator's initial questions, dated 25 January 2019. WhatsApp specifically confirmed, in this regard, that:

> *"WhatsApp Ireland is the controller for the internet-based messaging and calling service (the "Service") for EU users. WhatsApp Ireland is solely responsible for, and has the exclusive power to make, decisions about the purposes and means of processing of personal data of EU users. In particular, WhatsApp Ireland engages […] personnel located in Dublin, who perform various services for WhatsApp Ireland, including legal, law enforcement response, customer operations, information security, trust and safety, and training. In addition, WhatsApp Ireland is responsible for:*
>
> - *Making the Service available to users in the EU;*
> - *Setting policies that govern how EU user data is processed;*

- *Controlling access to and use of EU user data;*
- *Handling and resolving data-related inquiries and complaints regarding the Service from EU users whether directly or indirectly;*
- *Responding to requests for EU user data from law enforcement;*
- *Ensuring the Service's compliance with EU data protection laws and ongoing evaluation of the Service; and*
- *Guiding the development of products involving EU user data in accordance with EU data protection laws.*

10. WhatsApp further confirmed that "WhatsApp Ireland's single establishment with respect to personal data processed for the Service in the EU is located in Ireland."

Controllership and cross-border processing

11. Accordingly, it is clear, in circumstances where WhatsApp provides services to individuals across the EU (as detailed above) and engages in the processing of the personal data of individuals for the purposes of providing such services, that it is engaged in cross-border processing.

12. WhatsApp, in its response of 25 January 2019, as referred to above, has confirmed that it is the data controller in respect of the personal data of EU users. The Commission notes that this affirmation of controllership is contained in WhatsApp's Privacy Policy (second paragraph). Further the "Contact Information" section of WhatsApp's Privacy Policy also gives the contact address for the EU service as that of WhatsApp's office premises (which address, as detailed further below, is in Ireland).

The Commission's consideration of the factual position

13. As concerns whether WhatsApp is a data controller for EU users, it should be noted that there has been a course of historical and ongoing engagement, by WhatsApp, with the Commission's Consultation Unit (through which the Commission carries out its supervision function) dating back a number of years and predating the application of the GDPR. This engagement has been conducted in relation to the preparation and revision of WhatsApp's data protection policies as well as the handling of complaints, amongst other things. Having regard to these ongoing interactions, the Commission is satisfied that WhatsApp acts as the controller, determining the means and purposes of processing in respect of the personal data of individuals, in relation to the delivery of its services across the EU.

14. Further, as regards the requirement that, in order to come within the competency of the Commission as the lead supervisory authority, WhatsApp must demonstrate that it has either its single or main establishment in Ireland, the Commission confirms that WhatsApp, as controller for its cross-border processing activities, has its single establishment located in Ireland, with permanent office premises located at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2. The Commission is satisfied that WhatsApp's employees are, in ordinary course, based at these office premises.

15. Finally, and of significance, since 25 May 2018, a total of 88 complaints made against WhatsApp have been transmitted to the Commission by the supervisory authorities of Germany (the Federal authority acting on behalf of various regional authorities), the Netherlands, Austria, Spain, the United Kingdom, France, Finland and Poland, in circumstances where those authorities were acting as concerned supervisory authorities (insofar as they have received complaints from complainants). Those

complaints have been transmitted to the Commission on the basis that the Commission is the lead supervisory authority for WhatsApp. In this regard, the Commission notes that no supervisory authority to date has objected to such designation of the Commission as the lead supervisory authority in respect of the cross-border processing carried on by WhatsApp.

16. In all of the circumstances detailed above, the Commission is satisfied that, pursuant to Article 56(1) and Article 4(23)(a) of the GDPR, it is competent to act as the lead supervisory authority, for the purpose of the cross-border processing activities carried out by WhatsApp.

The Inquiry

17. The Commission notified WhatsApp of the commencement of an own-volition inquiry pursuant to Section 110 of the 2018 Act by way of letter dated 10 December 2018 ("the **Notice of Commencement**"). The Notice of Commencement identified the scope of the inquiry and put a series of questions to WhatsApp for the purpose of examining the matters in issue. For the avoidance of doubt, the inquiry was limited to WhatsApp's consumer services and does not relate to the "WhatsApp for Business" service. The term "the **Service**" is used throughout this Decision (and was used throughout the course of the within inquiry) to refer to WhatsApp's internet-based messaging and calling service. Similarly, the term "non-user" has been used throughout the within inquiry to denote an individual data subject who does not have an account with WhatsApp.

18. For the avoidance of doubt, the scope of the within inquiry is limited to an assessment of the extent to which WhatsApp complies with its transparency obligations pursuant to the GDPR. Considerations of WhatsApp's entitlement to rely on any particular legal basis when processing personal data fall outside of the scope of this inquiry. Accordingly, nothing in this Decision should be understood to represent confirmation of WhatsApp's entitlement to rely on any, or any particular, legal basis when processing personal data for the purposes of the Service.

19. By way of letter dated 25 January 2019, WhatsApp provided the Investigator with the information requested ("the **Response to Investigator's Questions**"). The Investigator made a subsequent request for clarification by way of email dated 8 March 2019. WhatsApp provided the clarification requested under cover of email dated 20 March 2019. Having considered the information furnished, the Investigator recorded her views and proposed findings in a draft inquiry report dated 30 May 2019 ("the **Draft Report**"). The Draft Report recorded the Investigator's understanding of the relevant factual background as well as her proposed findings as to whether or not an infringement of Articles 12, 13 and/or 14 of the GDPR had occurred/was occurring. WhatsApp responded to the contents of the Draft Report by way of letter dated 1 July 2019 ("the **Inquiry Submissions**"). Having taken account of the Inquiry Submissions, the Investigator concluded her final report on 9 September 2019 ("the **Final Report**"). The Investigator passed the Final Report, together with the inquiry file, to me on 9 September 2019. By way of letter dated 4 October 2019, I wrote to WhatsApp to notify it of the commencement of the decision-making stage.

Approach of the Decision-Maker

20. The Investigator took an approach whereby she reached fifteen separate conclusions (as summarised in Section G of the Final Report) following her assessment of the extent to which WhatsApp complies with the obligations set out in Articles 12, 13 and 14 of the GDPR. However, for ease of consideration

of the issues arising, I have adopted an approach based on an assessment of the issues arising under three core headings, as follows:

- *Part 1: Transparency in the context of non-users*

  Under this heading, I will consider the extent to which WhatsApp processes personal data in relation to non-users of the Service and whether any such processing gives rise to a requirement for WhatsApp to comply with the obligations set out in Articles 14 and 12(1) of the GDPR. The issues that I will consider under this heading correspond to the matters covered by Conclusions 1, 2 and 14 of the Final Report.

- *Part 2: Transparency in the context of users*

  Under this heading, I will consider the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of its processing of personal data relating to users of the Service. The issues that I will consider under this heading correspond to the matters covered by Conclusions 3 to 13 (inclusive) of the Final Report.

- *Part 3: Transparency in the context of any sharing of personal data between WhatsApp and the Facebook Companies*

  Under this heading, I will consider the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of any sharing of personal data between WhatsApp and the Facebook family of companies. For the purpose of this Decision, I will use the term "the **Facebook Companies**" to collectively refer to those members of the Facebook family of companies that process, for any purpose, personal data, whether as processors or as controllers, which have been shared with them by WhatsApp.

  The issues that I will consider under this heading correspond to the matters covered by Conclusion 15 of the Final Report.

Progression of the Decision-Making Stage

21. Upon completion of my assessment of the Final Report and inquiry file, I prepared the Preliminary Draft, recording my understanding of the relevant factual background and setting out my preliminary views, as to whether or not one or more infringements of the GDPR has occurred/is occurring. I provided WhatsApp with a copy of the Preliminary Draft as soon as it was ready, on 21 May 2020. Immediately afterwards, I prepared the Supplemental Draft, setting out my provisional views as to whether one or more corrective powers should be exercised in the event of my finding that an infringement of the GDPR has occurred/is occurring. As before, I provided WhatsApp with a copy of the Supplemental Draft as soon as it was ready, on 20 August 2020.

22. For the avoidance of doubt, the Supplemental Draft was prepared solely by reference to the provisional views and proposed findings recorded in the Preliminary Draft. In other words, I did not take account of the submissions that were received from WhatsApp in the intervening period (on 6 July 2020), in response to the Preliminary Draft. I informed WhatsApp of this by way of letter dated 20 August 2020 and expressly confirmed that I would take account of the submissions that had already been furnished, in response to the Preliminary Draft, and any submissions that might yet be

furnished, in response to the Supplemental Draft, when finalising the final versions of the Preliminary and Supplemental Drafts for circulation through the Article 60 process. WhatsApp furnished submissions in response to the Preliminary Draft under cover of letter dated 6 July 2020 ("the **Preliminary Draft Submissions**"). WhatsApp's submissions in response to the Supplemental Draft were furnished under cover of letter dated 1 October 2020 ("the **Supplemental Draft Submissions**").

23. As is apparent from the within Decision, the Preliminary Draft and the Supplemental Draft were combined into a single, composite draft decision, which was circulated to the other supervisory authorities concerned ("**CSAs**, each one being a "**CSA**"), in accordance with Article 60 of the GDPR, on 24 December 2020 ("the **Composite Draft**"). Given that the Service entails cross-border processing throughout Europe, all other Supervisory Authorities ("**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 Composite Draft:

    a. The German (Federal) SA raised an objection on 21 January 2021;
    b. The Hungarian SA raised an objection on 21 January 2021;
    c. The Dutch SA raised an objection on 21 January 2021;
    d. The Polish SA raised an objection on 22 January 2021;
    e. The French SA raised an objection on 22 January 2021;
    f. The Italian SA raised an objection on 22 January 2021;
    g. The Baden-Wurttemberg SA raised an objection on 22 January 2021; and
    h. The Portuguese SA raised an objection on 22 January 2021.

24. In addition, the following comments were exchanged:

    a. The Austrian SA exchanged a comment on 21 January 2021;
    b. The Dutch SA exchanged a comment on 21 January 2021;
    c. The Danish SA exchanged a comment on 22 January 2021;
    d. The Polish SA exchanged a comment on 22 January 2021;
    e. The Belgian SA exchanged a comment on 22 January 2021;
    f. The French SA exchanged a comment on 22 January 2021; and
    g. The Hamburg SA exchanged a comment on 22 January 2021.

25. Having considered the matters raised, the Commission, by way of a Composite Response Memorandum dated 1 April 2021, 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 Commission determined that it would not follow them. That being the case, the Commission referred the objections to the Board for determination pursuant to the Article 65(1)(a) dispute resolution mechanism. In advance of doing so, the Commission invited WhatsApp to exercise its right to be heard on all of the material that the Commission proposed to put before the Board. WhatsApp exercised its right to be heard by way of its submissions dated 28 May 2021 (the "**Article 65 Submissions**"). The Board adopted its Article 65 Decision on 28 July 2021 and notified it to the Commission and all other CSAs on 30 July 2021. **As per Article 65(1), the Board's decision is binding upon the Commission. Accordingly, and as required by Article 65(6) of the GDPR, the Commission has now amended its Composite Draft, 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 Composite Draft, 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 Commission.

Part 1: Transparency in the Context of Non-Users

Introduction

26. In this part of the Decision, I will consider the extent to which WhatsApp processes personal data in relation to non-users of the Service and whether any such processing gives rise to a requirement for WhatsApp to comply with the obligations set out in Articles 14 and 12(1) of the GDPR. The issues that I will consider under this heading correspond to the matters covered by Conclusions 1, 2 and 14 of the Final Report.

Relevant Provisions

27. Given that this part of the Decision entails a consideration of the obligations arising in the context of non-users of the Service, the relevant provisions of the GDPR are Article 14, read in conjunction with Article 12(1).

28. Article 14 of the GDPR concerns transparency in the context of personal data that have "*not been obtained from the data subject*". Where a data controller has obtained personal data from a source other than the data subject, Article 14 requires the data controller to provide the data subject with the information detailed in Articles 14(1) and 14(2).

29. Article 12(1) of the GDPR details the requirement for a controller to:

> *"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."*

30. Thus, while Article 14 addressees the specific information that must be communicated to data subjects, Article 12 addresses the *way* in which this information must be communicated.

The Inquiry Stage

The information sought and WhatsApp's response

31. Question 3 of Appendix A to the Notice of Commencement asked WhatsApp to confirm whether or not it processes personal data relating to non-users of the Service. Thereafter, Questions 9 – 15, inclusive, asked WhatsApp to demonstrate compliance with the various provisions of Article 14 and Article 12(1), in relation to the processing of any data relating to non-users of the Service.

32. WhatsApp stated, in its Response to Investigator's Questions, that it does not, as a data controller, process personal data relating to non-users of the Service. It clarified that, while it processes the telephone numbers of non-users of the Service, it does so:

*"as a processor on behalf of its EU users when providing its contact list feature (a popular voluntary feature of the Service) ("the **Contact Feature**")."*

33. WhatsApp further explained that:

"The Contact Feature allows users to request that [WhatsApp] access the phone numbers (no other details) in their address book for the purposes of determining which of their contacts is already using the Service. On behalf of such a user (e.g. "User A"), [WhatsApp] identifies for User A which of his/her contacts already use the Service and populates User A's contacts on the Service enabling User A to communicate with these users (the specific implementation of this varies slightly by device platform).

The Contact Feature is technologically possible only if [WhatsApp] accesses the phone numbers in User A's address book, which could in principle include the phone numbers of non-users. In such circumstances, [WhatsApp] will, in a very limited capacity as a processor for User A, process the phone numbers of such non-users (and no other details) on behalf of User A.

[WhatsApp] processes this data on behalf of User A for two purposes only. First, to establish which of User A's address book contacts also use the Service as part of the Contact Feature, and which are non-users. And secondly, in relation to those non-users' data, in order to quickly and conveniently update User A's contacts list on the Service as and when any of those non-users join the Service.

To ensure that it provides these services as a processor in line with the principles of privacy by design, [WhatsApp] only processes the non-users' phone numbers for the minimum time required to apply cryptographic lossy hashing, which is generally no more than a few seconds. This process generates a new value (known as a "lossy-hashed value") based on the phone number. It is this lossy-hashed value, and not the non-users' phone numbers, that is stored by WhatsApp for and on behalf of User A.

34. By way of a footnote (footnote 1) to the Response to Investigator's Questions, WhatsApp explained the applicable lossy hashing process as follows:

[redacted]

35. The Investigator, by way of a follow-up email dated 8 March 2019, requested clarification as to "*if and how a user can opt out of sharing their contacts, or categories of contacts, with WhatsApp*".

36. By way of email dated 20 March 2019, WhatsApp confirmed that "*EU users can choose whether or not to share their contacts with [WhatsApp] when registering for the [Service] … . They also have the ability to turn off sharing of contacts on or off at any time after registration via their device settings …*".

<u>The Questions for Determination and the Draft Report</u>

37. On the basis of the above, the Investigator sought to determine the answers to three specific questions, namely:

    a. Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?

    b. Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?

    c. In the event that either of the above questions is answered in the affirmative, does WhatsApp process the personal data as a processor (acting on behalf of an individual user who has activated the Contact Feature) or a data controller?

38. Having considered the position, the Investigator formed the preliminary view that any information processed by WhatsApp in relation to non-users (both before and after the lossy hashing process) constituted the personal data of those non-users. The Investigator formed that preliminary view by reference to:

    a. The definition of "personal data", as set out in Article 4(1) of the GDPR, which confirms that "*'personal data' means any information relating to an identified or* ***identifiable*** *natural person …"* (emphasis added);

    b. Recital 26 to the GDPR, which provides that *"[in order to] determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*"; and

    c. The judgment of the Court of Justice of the EU ("the **CJEU**") in *Breyer*[2].

39. The Investigator further formed the preliminary view that, when processing the personal data of non-users, WhatsApp did so as a controller, and not a processor. That preliminary view was based on:

    a. The definitions of "*controller*" and "*processor*", as set out in Articles 4(7) and 4(8) of the GDPR;

    b. The requirement, set out in Article 28(3) of the GDPR, for any processing (by a processor acting on behalf of a controller) to be governed by "*a contract or other legal act*";

    c. The application of the concept of "*data controller*", as considered by reference to the "*household exemption*" described in Article 2(2)(c) and Recital 18 of the GDPR and the judgments of the CJEU in the Facebook Fan Pages Case[3] and the Jehovah's Witnesses Case[4];

[2] *Breyer v Bundesrepublik Deutschland* (Case C-582/14, judgment delivered on 19 October 2016) ("**Breyer**")
[3] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Case C-210/16, judgment delivered on 5 June 2018) ("the **Facebook Fan Pages Case**")
[4] *Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta* (Case C-25/17, judgement delivered on 10 July 2018) ("the **Jehovah's Witnesses Case**")

d. The view of the Article 29 Working Party, as set out in Opinion 1/2010 on the concepts of "controller" and "processor"[5];

e. The fact that a user cannot choose to limit the Contact Feature to apply only to the contact information of other users of the Service; and

f. The benefit, to WhatsApp, of the processing and a doubt as to whether the storage of non-user numbers (albeit in the form of hash values) was necessary for the purpose of the Contact Feature.

WhatsApp's Response to the Draft Report

40. WhatsApp, by way of its Inquiry Submissions, disagreed with the Investigator's views and asserted that:

a. "*WhatsApp has no ability to link a non-user's phone number to a specific individual – even if it were possible to do so during the few seconds such phone numbers are held*";

b. "*The effect of the lossy-hashing procedure is that WhatsApp cannot reverse engineer the value into the original phone number … It is computationally impossible. At most, WhatsApp could possibly link the value back to a group of up to sixteen different possible phone numbers. In short, once the lossy-hashing process has been applied, WhatsApp loses the ability to reidentify the specific non-user's phone number. The information is genuinely and irreversibly anonymous in nature*";

c. There are no reasonable means available to WhatsApp that would enable it to associate the phone number with an identifiable natural person; and

d. The judgment in *Breyer* is not applicable in circumstances where "*no established means or channels are available to enable WhatsApp to ascertain the identity of the owner of the non-user phone number, and certainly none are identified in the Draft Report*".

41. In relation to the Investigator's proposed finding concerning WhatsApp's status when processing non-user data, WhatsApp again disagreed with the Investigator's views and asserted that:

a. The initial action/decision to process data (by way of the Contact Feature) is made by the uploading user;

b. The Investigator appeared to have ignored the fact that this aspect of the Service is technologically possible only if WhatsApp accesses all of the phone numbers in an uploading user's address book. The Investigator's suggestion, in this regard, that WhatsApp should allow an opt-out in respect of the sharing of non-user contacts ignores this fact as well as the purpose of importing contacts;

[5] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted 16 February 2010 (00264/10/EN WP 169) ("**Opinion 1/2010**").

c. In any event, an opt-out would be unworkable in practice in circumstances where "*users generally have no way of knowing which of their contacts currently use the WhatsApp service prior to uploading their contacts, and so would have no way of knowing which friends' contact information they were opting-out from sharing*";

d. In addition to the above, any approach that does not involve the storage of lossy-hashed non-user contacts would (i) impose huge engineering costs on WhatsApp; and (ii) significantly degrade the experience of WhatsApp users by slowing down the Service and consuming excessive bandwidth on users' phones;

e. WhatsApp cannot be said to exert control over the processing of non-user data when its capacities are limited to storing and deleting (undecipherable hashes of) that data. WhatsApp submitted, in this regard, that it is clear that the uploading user exerts influence over the processing of personal data for their purposes, and so participates in determining the purposes and means of that processing;

f. The Investigator failed to cite any evidence in support of her conclusion that the storage of non-user data allegedly served WhatsApp's purposes more than those of the uploading user. WhatsApp submitted, in this regard, that the purpose of the Contact Feature is to "*enable [the] user to use WhatsApp as a means of readily contacting his or her friends, regardless of whether those friends are current users of WhatsApp or may be users in the future*". According to WhatsApp, this serves the user's interests.

42. To support its position, WhatsApp provided some additional information to explain the manner in which the lossy-hashed values are used to "*speedily update WhatsApp users' contacts on their behalf when their friends join the service*". WhatsApp explained[6] that the applicable process, when a new user joins the Service and submits his/her phone number as part of the registration process, is as follows:

a. "*The phone number of the new user undergoes the same lossy-hashing method described [as before];*

b. *WhatsApp checks if the resulting hash value is already contained in the stored list generated from non-users' phone numbers. This list links each stored hash value to the WhatsApp user(s) who uploaded the non-user phone number from which that hash was generated. As a result, by checking this list, WhatsApp can identify all existing WhatsApp users who may potentially have uploaded this new users' phone number previously (and so may potentially have this new user in the contact list);*

c. *However, because each stored hashed value can be linked to as many as sixteen different phone numbers, it is impossible for WhatsApp to conclude with certainty as a result of this process which users will indeed have the new user in their contact list;*

d. *To address this, a request is sent – to users' devices, not the users themselves – to the full set of users WhatsApp has established may have the new user in their contact list. Given the*

[6] The Inquiry Submissions, paragraph 3.4

nature of the lossy-hashed value (i.e. because the same value can be generated from hashing sixteen different numbers), WhatsApp necessarily over-notifies in this regard, albeit the hash comparing process mitigates the amount of this over-notification;

e. *Upon receiving this request, the app on each user's device will verify if the new user's phone number is indeed contained in the contact list on that device; and*

f. *If the new user is indeed listed on the device's contact list, their listing will be updated in the app to display to the relevant user the fact that this new user can now be contacted through WhatsApp."*

43. Having considered the Inquiry Submissions, the Investigator finalised her report, concluding that the information processed by WhatsApp in relation to non-users remains, at all times, the personal data of those non-users. She further found that, when processing this data, WhatsApp did so as a controller and not a processor.

The Decision-Making Stage

Relevant Background and Findings of Fact

44. Having assessed the information collected during the inquiry stage, I summarised, in the Preliminary Draft, the background information that I considered to be relevant and by reference to which I proposed to consider the issues arising. By way of the Preliminary Draft Submissions, WhatsApp corrected certain information that had previously been provided and added further information that had not been previously provided. The following now represents the amended factual framework upon which I propose to base my assessment of the issues arising, for the purpose of this Part 1:

a. The Service includes an optional Contact Feature that allows a user to request that WhatsApp access the phone numbers stored in the address book of the individual user's device. The stated purpose of the Contact Feature is to enable WhatsApp, on behalf of a user, to identify which of that user's contacts already use the Service and to populate any user contacts on the Service, thereby enabling the requesting user to communicate with his/her contacts via the Service.[7]

b. While an address book will contain various different types of information, such as names, phone numbers and email addresses, WhatsApp only processes the mobile phone numbers of the user's contacts for the purpose of the Contact Feature.[8]

c. Given that an individual's address book may contain the contact details of both users and non-users, WhatsApp may end up accessing the numbers of both users and non-users of the Service when it accesses an individual's address book for the purpose of the Contact Feature. The reasons for this are twofold:

I. firstly, this processing is necessary to establish which of the requesting user's contacts are already users of the Service (so as to enable the updating of the user's contacts on the Service);

[7] Per the "Information We Collect" section of the Privacy Policy and the Contact Feature Pop-Up
[8] Response to Investigator's Questions (response to Question 3a.)

II. secondly, in relation to the phone numbers of any non-users, WhatsApp processes this information so as to be able to quickly and conveniently update the requesting user's contacts list as and when any of those non-users join the Service.[9]

d. When processing the phone numbers of non-users, WhatsApp typically does so for no more than a few seconds prior to their deletion. This includes the time it takes to (i) access all mobile phone numbers on a user's device, (ii) transfer those numbers, in unhashed form, to WhatsApp's servers, (iii) generate irreversible hashes of the non-user numbers once they reach these servers (which itself takes a matter of microseconds), and (iv) delete the underlying phone numbers[10]. The applicable hashing process may be summarised as follows:

I. [redacted]

II. [redacted]

III. [redacted][11]

e. The effect of the lossy hashing process is that WhatsApp cannot reverse engineer the Lossy Hash into the original non-user's phone number.[12] Further, the same Lossy Hash can be generated from a minimum of sixteen different phone numbers[13].

f. Lossy Hashes are stored in a list ("the **Non-User List**") on WhatsApp's servers[14]. Each Lossy Hash is linked, in the list, to the user who uploaded the original non-user's number.[15]

g. When a new user joins the Service, his/her phone number is lossy-hashed in accordance with the process outlined at d. above[16]. The resulting Lossy Hash is compared to the hash values stored in the Non-User List[17]. The purpose of this exercise is to update the contacts of any existing users whose address books previously included the new user (albeit at a point in time when the new user was a non-user)[18].

[9] Response to Investigator's Questions (response to Question 3a.)
[10] The Preliminary Draft Submissions, paragraph 3.3 and the Example provided
[11] Response to Investigator's Questions (response to Question 3a.), as supplemented/amended by the Preliminary Draft Submissions (step 2 of the Example set out at paragraph 3.3)
[12] The Inquiry Submissions, paragraph 3.3
[13] The Preliminary Draft Submissions (steps 2 and 3 of the Example set out at paragraph 3.3 and footnote 22)
[14] The Inquiry Submissions, paragraph 3.4(ii)
[15] The Inquiry Submissions, paragraph 3.4(ii)
[16] The Inquiry Submissions, paragraph 3.4(i)
[17] The Inquiry Submissions, paragraph 3.4(ii)
[18] The Inquiry Submissions, paragraph 3.4

h. If the Lossy Hash generated from the new user's number is matched with a Lossy Hash already stored in the Non-User List, this does not mean that WhatsApp can identify which users have the new user's mobile phone number in their address books. As each stored Lossy Hash can be theoretically linked to a minimum of sixteen different phone numbers, it is impossible for WhatsApp to conclude, as a result of this process, which of the possible matches have a particular new user's number in their contacts. It may even be the case that none of the matches have the new user's number in their contacts[19]. The utility of the Non-User List is not that it enables precise matching of new-users to existing users but, rather, it "very significantly" reduces the number of devices that WhatsApp needs to notify when a new user joins the Service; instead of having to issue notifications to all WhatsApp users, it is only necessary for notifications to issue to those potential matches identified in the Non-User List[20].

i. In order to establish which users (if any) have the new user in their contacts, WhatsApp sends a notification to the devices of any linked users (i.e. any users that were identified as potentially having the new user in their contact lists pursuant to the step outlined at g. above)[21]. As clarified by WhatsApp, by way of the Preliminary Draft Submissions, the notification does not include the Lossy Hash itself, which plays no further role in the process after assisting to reduce the number of devices WhatsApp needs to notify. Instead, the notification includes [redacted] of the new user's phone number ("the **Notification Hash**"), which is only generated after the new user signs up to use the Service[22].

j. Upon receipt of the notification, the relevant device will compute the Notification Hash for every contact it has stored locally and check whether any of those hashes match the Notification Hash received. If a match is found, the device will send a sync request (with the mobile phone number in unhashed form) to the WhatsApp server. WhatsApp will then update the WhatsApp contacts on behalf of those users that actually have the new user's phone number in their mobile phone address book, so that the new user is then their WhatsApp contact[23].

The Questions for Determination

45. The above gives rise to three specific questions for determination, namely:

a. Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?

b. Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?

c. In the event that either of the above questions is answered in the affirmative, does WhatsApp process the personal data as a processor (acting on behalf of an individual user who has activated the Contact Feature) or a data controller?

[19] The Preliminary Draft Submissions (step 4 of the Example set out at paragraph 3.3)
[20] The Preliminary Draft Submissions (step 5 of the Example set out at paragraph 3.3)
[21] The Inquiry Submissions, paragraph 3.4(iv)
[22] The Preliminary Draft Submissions (step 5 of the Example set out at paragraph 3.3)
[23] The Inquiry Submissions, paragraphs 3.4(v) and 3.4(vi) and the Preliminary Draft Submissions (step 5 of the Example set out at paragraph 3.3)

46. I propose to firstly address questions (a) and (b), above, given that the third question will only require determination in the event that I find that the phone number of a non-user constitutes the personal data of that non-user (either before or after the lossy hashing process).

Legal Analysis – Questions (a) and (b)

47. To begin, it is useful to recall the definition of "personal data", as set out in Article 4(1) of the GDPR, as follows:

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

48. It is therefore clear that, in order for information to constitute "personal data", it must relate to an "identified" or "identifiable" natural person. While it will usually be self-evident if a data subject has been "identified", the meaning of "identifiable" and, in particular, the circumstances in which a person might be "indirectly" identified, requires further consideration.

49. Turning, firstly, to Recital 26 of the GDPR, which acts as an aid to the interpretation of Article 4(1), that provision clarifies that:

> *"… (t)o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."*

50. Thus, when determining whether or not a natural person is "*identifiable*", it is necessary to:

    a. Firstly, identify the ways in which a person might be identified, directly or indirectly, either by the controller or by another person; and

    b. Then, consider whether the mechanisms identified above are "*reasonably likely*" to be used, by the controller "*or by another person*", taking account of all objective factors such as any associated cost, the time required for identification, the available technology and technological developments.

Opinion 4/2007

51. The provisions discussed above were considered by the Article 29 Working Party in its "Opinion 4/2007 on the concept of personal data"[24] ("**Opinion 4/2007**"). While Opinion 4/2007 addresses the

[24] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted 20 June 2007 (01248/07/EN WP 136) ("**Opinion 4/2007**")

issue by reference to the definition of "*personal data*" set out in Article 2(a) of Directive 95/46/EC[25] ("the **Directive**"), that definition is materially identical to the definition set out in Article 4(1) of the GDPR. I further note that the text of the accompanying recital (Recital 26 of the Directive) is very similar to the text of Recital 26 of the GDPR. While I am further cognizant of the facts that (i) Opinion 4/2007 is non-binding; and (ii) the Article 29 Working Party was replaced, pursuant to Article 68 of the GDPR, by the European Data Protection Board on 25 May 2018, the views expressed in Opinion 4/2007 nonetheless provide a helpful analysis of the factors that should be taken into account when considering if a natural person is "*identifiable*".

52. Opinion 4/2007 firstly notes, in this regard, that:

> *"… a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group.* ***Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able").***" [emphasis added]

53. Opinion 4/2007 further observes that:

> *"As regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person,* ***that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others****."* [emphasis added]

54. Considering, specifically, the "*means to identify*" aspect of Recital 26, Opinion 4/2007 considered that:

> *"One relevant factor … for assessing "all the means likely reasonably to be used" to identify the persons will in fact be the purpose pursued by the data controller in the data processing. National Data Protection Authorities have been confronted with cases where, on the one hand, the controller argues that only scattered pieces of information are processed, without reference to a name or any other direct identifiers, and advocates that the data should not be considered as personal data and not be subject to the data protection rules. On the other hand, the processing of that information only makes sense if it allows identification of specific individuals and treatment of them in a certain way.* ***In these cases, where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means "likely reasonably to be used" to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms. Therefore, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules****."* [emphasis added]

55. By contrast, Opinion 4/2007 also considered the position where steps have been taken to remove the possibility of identification of the data subject:

> *"In other areas of research or of the same project, re-identification of the data subject may have been excluded in the design of protocols and procedure, for instance because there is no*

[25] 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 ("the **Directive**")

therapeutical aspect involved. For technical or other reasons, there may still be a way to find out to what persons correspond what clinical data, but the identification is not supposed or expected to take place under any circumstance, and appropriate technical measures (e.g. cryptographic, irreversible hashing) have been put in place to prevent that from happening. In this case, even if identification of certain data subjects may take place despite all those protocols and measures (due to unforeseeable circumstances such as accidental matching of qualities of the data subject that reveal his/her identity), the information processed by the original controller may not be considered to relate to identified or identifiable individuals taking account of all the means likely reasonably to be used by the controller or by any other person. …"

Relevant Caselaw

56. Noting the above, I must finally consider how these principles have been interpreted by the CJEU in those cases that required consideration of the circumstances in which an individual might be said to be "indirectly" identifiable. I note, in this regard, that it has been established that:

    a. "*the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number … constitutes 'the processing of personal data wholly or partly by automatic means'*"[26];

    b. static IP addresses "*are protected personal data because they allow those users to be precisely identified*"[27]; and

    c. "*[an exam] candidate at a professional examination is a natural person who can be identified, either directly, through his name, or indirectly, through an identification number, these being placed either on the examination script or on its cover sheet*."[28]

57. Turning to the *Breyer* judgment[29], the Court, in this case, considered a scenario whereby an online media service provider ("**Party A**") retained log files of certain information pertaining to access requests made to its web pages/files. The log files included the IP address of the computer from which access was sought. The information required to identify an individual user, however, was held by a third party (the user's internet service provider) ("**Party B**").

58. A further complicating factor in the case was the fact that the IP address in question was a 'dynamic' IP address, rather than a 'static' one. As set out above, it had been previously established[30] that a static IP address constitutes the personal data of the user because it allows the user to be precisely identified. Unlike a static IP address, however, a dynamic IP address changes each time there is a new connection to the internet. Accordingly, a dynamic IP address does not enable a link to be established between a given computer and the physical connection to the network used by the internet service provider.

---

[26] *Lindqvist* (Case C-101/01, judgment delivered by the CJEU on 6 November 2003) ("**Lindqvist**")
[27] *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Case C-70/10, judgment delivered by the CJEU on 24 November 2011) ("**Scarlet Extended**")
[28] *Nowak v Data Protection Commissioner* (Case C-434/16, judgment delivered by the CJEU on 20 December 2017) ("**Nowak**")
[29] *Breyer v Bundesrepublik Deutschland* (Case C-582/14, judgment delivered on 19 October 2016) ("**Breyer**")
[30] *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Case C-70/10, judgment delivered by the CJEU on 24 November 2011) ("**Scarlet Extended**")

59. Accordingly, the data stored by Party A did not enable the user to be directly identified; Party A could only do so if the information relating to the user's identity was communicated to it by Party B. In the circumstances, a question arose as to whether or not the contents of the log files constituted the personal data of the user. The answer to this question depended on whether the user was "identifiable".

60. Considering the position, the Court firstly observed that a dynamic IP address does not constitute information relating to an 'identified natural person' because that information does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer. The Court observed, however, that the inclusion of the word 'indirectly' in the definition of "personal data" suggested that, in order for information to constitute "personal data", it is not necessary that that information alone enables the data subject to be identified.

61. Turning to Recital 26 of the Directive, the Court firstly noted that this required account to be taken of "*all the means likely reasonably to be used either by the controller or by any other person to identify*" the said person. The Court observed that this particular wording suggested that, in order for information to constitute "personal data", it is not required that "*all the information enabling the identification of the data subject must be in the hands of one person*".

62. Accordingly, a determination was required in relation to whether or not the possibility that the dynamic IP address held by Party A might be combined with additional data held by Party B constituted a "*means likely reasonably to be used*" to identify the data subject. The Court observed that this would not be the case if the identification of the data subject, in this manner, was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appeared, in reality, to be insignificant.

63. Considering this question in the particular circumstances of the case, the Court noted that German law (the applicable national law, for the purpose of the assessment) did not permit Party B to directly transmit the additional data that would enable the identification of the data subject to Party A. The Court observed, however, that legal channels existed such that Party A could contact the competent authority (to report, for example, a cyber-attack), so that the competent authority could take the steps necessary to obtain the identifying information from Party B so as to commence criminal proceedings. In this way, the data subject would be identified as a result of the combination, by the competent authority, of the information held by Party A with the identifying data held by Party B.

64. On the basis of the above, the Court concluded that Party A had the means "likely reasonably to be used" in order to identify the data subject, with the assistance of other persons, namely the competent authority and Party B, on the basis of the IP addresses stored in Party A's log files.

65. Accordingly, the Court found that a dynamic IP address, registered by Party A when a person accesses its website, constitutes personal data, in the hands of Party A, where Party A has the legal means available to it to enable the identification of a data subject by way of additional data held, about that data subject, by Party B.

<u>The Preliminary Draft and the Proposed Findings – Questions (a) and (b)</u>

66. Applying the above to the within inquiry, I proposed findings, in the Preliminary Draft, that the phone number of a non-user constitutes the personal data of that non-user both before and after the lossy hashing process.

67. In relation to the position before the lossy hashing process, my view was that a mobile phone number is no different in quality to a static IP address (as considered in *Scarlet Extended*), a (landline) telephone number (as considered in *Lindqvist*) or an identification number (as considered in *Nowak*). As detailed above, each of these factors have been found, by the CJEU, as being capable of enabling the indirect identification of a natural person. Accordingly, and adopting the reasoning of the CJEU in the cases discussed above, I formed the preliminary view that the phone number of a non-user constitutes the personal data of that non-user in circumstances where the non-user can be indirectly identified by reference to his/her phone number.

68. In relation to the status of the phone number of a non-user, after the lossy hashing process, my proposed finding, in this regard, was informed by the purpose of the Contact Feature (which is designed to "*quickly and conveniently*" update the relevant users' contacts lists "*as and when any of those non-users join the Service*"). I noted, in this regard, that WhatsApp is able to achieve this objective because it stores Lossy Hashes in combination with the derivative user contact in the Non-User List. As a result, WhatsApp can update user contacts to include the details of a new user by:

    a. Firstly narrowing down the users who might have the new user in their address books (albeit originally as a non-user); and

    b. Then verifying, from the narrowed-down list of possible matches, those users who actually have the new user in their address books.

69. On the basis of the above, it seemed to me that the purpose of the processing of non-user contacts (including the application of the lossy hashing process) implied the identification of individuals. In other words, by lossy hashing non-user contacts and storing the resulting Lossy Hash in combination with the number of the derivative user, WhatsApp is able to "quickly and conveniently" match up new users (who were previously non-users) with their contacts. In the circumstances, I recalled the view expressed by the Article 29 Working Party in Opinion 4/2007, that: "*to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms*".

70. I further noted that the circumstances appeared to be very similar to those outlined in *Breyer*. Here, I observed, WhatsApp is ultimately able to match new users with their friends if the new user was previously a non-user whose number was lossy-hashed and stored in the Non-User List in combination with the details of the derivative user contact. On this basis, it appeared to me that WhatsApp could, if requested to do so by a competent authority (such as An Garda Síochána, the Irish competent authority), achieve the indirect identification of the non-user concerned by subjecting any mobile phone number that might be provided by the competent authority to the new user process with a view to identifying those existing users who have the number in their address books. This would then enable the competent authority to contact the identified users to request that they identify the name of their non-user contact.

<u>WhatsApp's Response to the Proposed Findings – Questions (a) and (b)</u>

71. By way of the Preliminary Draft Submissions, WhatsApp disagreed with the proposed findings. It firstly submitted, in this regard, that the purpose and technical limitations of the lossy hashing process were not fully appreciated and reflected in the Preliminary Draft. WhatsApp submitted, in this regard, that:

    a. "*the purpose of the processing is not to enable WhatsApp to identify non-users; instead, its aim and effect is to enable WhatsApp (when directed to do so by existing users) to facilitate prompt and efficient connectivity for existing users when new users join the [Service] … To the extent that WhatsApp engages in any processing of data in connection with the mobile phone numbers of non-users, that processing is undertaken exclusively for the purpose of facilitating this user-to-user connectivity*."[31]

    b. The Lossy Hash itself is used to ensure that the process can be conducted in a resource-efficient manner (e.g. by reducing the impact on user devices). It does this by enabling WhatsApp to only have to send notifications, using the Notification Hash, to a limited group of users, as identified by the Non-User List, as opposed to all WhatsApp users.[32]

    c. Based on how WhatsApp's systems currently operate, it is not technically feasible for it to extract unhashed non-user numbers from the hashing process during the transient period it processes them. In order to even access such unhashed non-user numbers, WhatsApp would need to design and implement code changes in order to process and log additional information to that which it does currently[33].

72. WhatsApp further submitted that the Preliminary Draft failed to consider the unique circumstances of *Breyer* and failed to explain how the principles established in that case could support the proposed findings;

    a. "*The conclusion that the processing of the [Lossy Hash] by WhatsApp amounts to the processing of personal data of non-users does not reflect the fact that what constitutes personal data is contextual and highly fact-specific. What is personal data in one person's hands will not necessarily be personal data in another person's hands; and whether indirect identification can be achieved will depend on the factual circumstances at hand*[34]."

    b. "*There is no third party from whom WhatsApp could, using reasonable means (or indeed at all), source information in order to combine it with [Lossy Hashes] (or the unhashed mobile phone numbers, given the manner in which WhatsApp processes them …) so as to identify an individual." "An Garda Síochána do not have the power under Irish law to compel WhatsApp to undertake the actions envisaged by the Commission's hypothetical scenario and, even if it did, the exercise of those powers would not result in WhatsApp itself being able to identify any non-user*"[35]

[31] The Preliminary Draft Submissions, paragraph 3.4(A)
[32] The Preliminary Draft Submissions, paragraph 3.4(A)
[33] The Preliminary Draft Submissions, paragraph 3.10
[34] The Preliminary Draft Submissions, paragraph 3.4(B)
[35] The Preliminary Draft Submissions, paragraphs 22(B), 25 and 26

c. "*The Commission's conclusions would produce illogical consequences whereby a person processing particular information from which an individual cannot be identified will be processing personal data … simply because a third party, acting entirely of its own volition, unilaterally decides to provide that person with other information so that further processing can take place which may ultimately enable that third party to then identify a person. Such an outcome is clearly not consistent with the rationale of Breyer and is irreconcilable with the EU law principle of proportionality*[36]."

73. WhatsApp further submitted that the proposed findings were not consistent with Recital 30 of the GDPR or the fact that WhatsApp did not collect the information necessary to identify the non-user data subjects:

a. The Commission "*has not explained why unhashed non-user mobile phone numbers in WhatsApp's hands (for – at most – a few seconds only and with no access to other identifying information) could comprise personal data*". Such a conclusion is not supported by the cases relied upon, nor can it be reconciled with Recital 30. Further, WhatsApp does not have either the technical nor lawful means to identify non-users during the very short period it processes these mobile phone numbers. "*In any event, it is not consistent with the proportionality principle to conclude that an entity which processes a mobile phone number for a matter of seconds can be said to be processing "personal data". That point applies with particular force where, as here, that momentary processing is itself undertaken solely for the purpose of enabling a hashing process that conclusively prevents any subsequent identification of the original mobile phone number (still less the owner of the number)*[37]."

b. Recital 30 of the GDPR makes it clear that online identifiers, such as an IP address, do not automatically enable the identification of individuals, and it may be necessary to combine those identifiers with other unique identifiers to enable the individual to be identified. If an online address such as an IP address is not automatically to be treated as data that enables the identification of an individual, then it must logically follow that a mere mobile phone number does not automatically enable such identification either. The implication of Recital 30 is that, in the case of online identifiers, you need to have access to other identifying information to be in a position where you can be said to be processing personal data. The same must logically follow in respect of mobile phone numbers[38].

c. In all of the cases relied upon by the Commission, the controller had access to other information enabling the ready identification of the person to whom the data related, and/or the nature of the relevant data processing was such that it would have enabled third parties to readily identify the person to whom the data related[39]. None of the judgments cited in the Preliminary Draft support the conclusion that a standalone mobile phone number – processed as it is for a brief moment and in circumstances where no identification of the non-user through other means is envisaged or even practically possible – can be treated as personal data for the purposes of Article 4(1)[40].

[36] The Preliminary Draft Submissions, paragraphs 3.22(C)
[37] The Preliminary Draft Submissions, paragraph 3.6
[38] The Preliminary Draft Submissions, paragraph 3.7
[39] The Preliminary Draft Submissions, paragraph 3.8
[40] The Preliminary Draft Submissions, paragraph 3.9

74. WhatsApp finally submitted that the proposed findings could not be reconciled with the principle of proportionality:

    a. *"… even if WhatsApp could be said to be processing personal data during this momentary period, that processing would itself be so transient and trivial that, by itself, it could not found an obligation to notify non-users; any other conclusion would of necessity fall foul of the proportionality principle engaged in the application of Article 14 GDPR*.[41]"

    b. The application of the proportionality principle leads to the conclusion that the processing of unhashed mobile phone numbers by WhatsApp does not amount to the processing of personal data because of (i) the transient nature; (ii) the fact that the processing is limited to the non-user's mobile phone number; and (iii) the processing is undertaken merely as a precursor to a hashing process resulting in the irreversible anonymization of the number and designed to enable user-to-user connectivity (as opposed to the identification of non-users). In the circumstances, it would not be proportionate to treat the processing as amounting to the processing of personal data. This is particularly the case given the lack of any meaningful privacy consequences for non-users[42].

Analysis and Discussion: Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?

75. In the Preliminary Draft, I proposed a finding that the phone number of a non-user, prior to the application of the lossy hashing process, constitutes the personal data of that non-user on the basis that such a number constitutes "information relating to an identified or identifiable natural person". WhatsApp disputed this proposed finding on a number of grounds, as summarised above. The central tenet of WhatsApp's position is that the mobile phone number of a non-user, in the absence of further information concerning the identity of that non-user, does not enable the identification of the non-user concerned.

76. Article 4(1) defines "personal data" as meaning "*any information relating to an identified or identifiable natural person*". It clarifies that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

77. The above definition makes it clear that, firstly, the concept of "personal data" is highly dependent on context, rather than the application of fixed rules. Secondly, the inclusion of the possibilities that an individual might not just be "identified", but "identifiable", and that such identification might be either "direct" or "indirect", clearly indicates that the legislature intended to ascribe a broad meaning to the term "personal data". Thirdly, the use of the words "(i)n particular", prior to the list of sample identifiers, makes it clear that the list provided is not exhaustive and that there are potentially innumerable ways in which an individual might be said to be identified or identifiable.

[41] The Preliminary Draft Submissions, paragraph 3.4(C)
[42] The Preliminary Draft Submissions, paragraph 3.11

78. Recital 26, which acts as an aid to the interpretation of Article 4(1), provides further indication as to the circumstances in which an individual might be considered to be "identifiable":

    a. "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*".

    b. "*To determine whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*."

79. It seems to me that Recital 26 envisages a risk-based approach to the question of whether, in any given set of circumstances, an individual might be said to be "identifiable"; it requires the potential risk of identification to be assessed by reference to "all of the means reasonably likely to be used", either by the controller or by a third party, and for those identified "means" to be assessed by reference to the factors that might help or hinder identification by way of those identified "means".

80. Applying the above to the circumstances under assessment, I firstly note that WhatsApp processes the following information concerning non-users:

    a. The mobile phone number of the non-user; plus

    b. The name and mobile phone number of the user from whose address book the non-user's number has been collected.

81. In terms of what this information discloses about the non-user concerned, I note that it enables me to:

    a. know that the individual concerned is not a user of the Service; and

    b. infer the likely existence of some sort of relationship between the individual concerned and the associated user.

82. The question for determination, therefore, is whether or not the mobile phone number of a non-user, either by itself or with the other information described in paragraph 80, above, enables the non-user concerned to be identified, or at least capable of being identified, either directly or indirectly. When considering this, I must take account of "all the means reasonably likely to be used … either by the controller or by another person to identify [the individual] directly or indirectly". When assessing whether the "means" identified are "reasonably likely to be used" to identify the individual concerned, I must take account of all objective factors, such as the cost involved and time required to achieve identification as well as the available technology and technological developments.

83. Considering, firstly, whether or not the non-user can be identified, or rendered capable of identification, directly or indirectly, from his/her mobile phone number, I note that a mobile phone number is somewhat unique in that it provides a direct route to, and a means of communicating with,

the individual concerned. In the circumstances, it is possible that the individual concerned could be considered to be "identifiable" by several means, including:

a. WhatsApp, or any third party, could dial the non-user's mobile phone number to make further enquiries as to the identity of the non-user concerned;

b. WhatsApp, or any third party, could access the non-user's voicemail greeting to see if the individual has identified himself/herself in that greeting;

c. WhatsApp, or any third party, could carry out internet / social media searches, using the non-user's mobile phone number as the search criterion;

d. WhatsApp, or any third party, could contact the associated user to make further enquiries as to the identity of the non-user concerned;

e. WhatsApp, or any third party, could carry out internet / social media searches, using the non-user's mobile phone number, in conjunction with the name and mobile phone number of the associated user, as the search criteria.

84. I note that there are no barriers to the use of the "means" identified above and that they represent options that are readily available to any interested party. Further, they do not entail a significant investment of time or money and neither do they require any particular technological expertise or equipment. Accordingly, I do not think that the "means" identified could be said to require a disproportionate effort, in terms of time, cost or man-power. I consider, therefore, that they are means "reasonably likely to be used" to identify the non-user concerned.

85. For the avoidance of doubt, I acknowledge that the identified options only provide for the *possibility*, rather than the guarantee of identification of the non-user concerned. My view, in this regard, is that neither Article 4(1) nor Recital 26 require the guarantee of identification in the context of an assessment as to whether or not an individual might be "identifiable". As already observed, Article 4(1) and Recital 26 envisage a risk-based approach to the possibility of identification. This risk-based approach is reflected in *Breyer*, where the Court observed that, when considering if a particular means constituted "a means likely reasonably to be used to identify the data subject":

> *"… that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power,* ***so that the risk of identification appears in reality to be insignificant****."* [emphasis added][43]

86. The language used by the CJEU, above, strongly supports the proposition that the assessment of whether an individual might be identifiable does not require a conclusion that an individual is either absolutely identifiable or absolutely not identifiable. Rather, it is sufficient for the assessment to discount the possibility of identification by concluding that risk of identification, as assessed, appears to be "insignificant".

[43] *Breyer*, paragraph 46

87. In the context of the within assessment, my view is that the risk of identification, by way of the "means" outlined at paragraph 83 above, cannot be described as "insignificant". In my view, it is just as likely as not that an individual might be identified by way of the "means" outlined above, given:

    a. The unique nature of a mobile phone number, being both a piece of information as well as a conduit by which direct contact can be made with the individual concerned; and

    b. As regards the possibility of identification by way of internet / social media searches, the ease of access to, and proliferation of, platforms and apps that are dedicated to facilitating communication and the sharing of information between individuals, the increasing number of individuals that are using such platforms and apps and the fact that individuals can reach a potentially infinite audience through these platforms and apps. The ease with which individuals can share, with a potentially infinite audience, information about both themselves and others, including, for example, mobile phone numbers, makes it possible for individuals to be identified through the traces of their activities which are left online, including where they have posted, shared or otherwise disclosed a mobile phone number.

88. For the sake of completeness, I note that there is one avenue by which the identity of any non-user could be ascertained in each and every case, namely the combination of the non-user mobile phone number with the corresponding name and address held by the relevant telecoms provider. I note that, similar to the position in *Breyer*, such a combination would only appear to be possible by way of the intervention of a third party such as An Garda Síochána (the Irish competent authority) in a case whereby WhatsApp might seek to identify the owner of the non-user number in connection with a criminal complaint. In terms of the feasibility of such a possibility, WhatsApp is no different to any other data controller in that it may find itself the target of criminal activity, including cybercrime, from time to time. It stands to reason that the reporting of any such criminal activity to An Garda Síochána may necessitate the sharing of information in relation to the individuals potentially responsible with a view to ultimately identifying those responsible. It is possible for such information to include a mobile phone number that WhatsApp has not, by way of its own records, been able to associate with an existing user. In such a scenario, the owner of the non-user mobile phone number held by WhatsApp could be identified with the addition of the name of the relevant registered owner of the mobile phone number, as held by the relevant mobile phone network provider with which the phone number is registered, through the intervention of An Garda Síochána.

89. As part of my assessment of this issue, I have also considered the possible consequences of a contrary finding, whereby, as advanced by WhatsApp, the mobile phone number of a non-user does not constitute the "personal data" of the individual concerned. Such an outcome would mean that WhatsApp (or, indeed, any entity) would be free to process this information without limitation; WhatsApp could legitimately share the information with any entity it wished, for any reason it wished, and any occurrence of unintended disclosure or interception would be entirely inconsequential. In order for such a position to be consistent with the GDPR, it would be necessary to classify a mobile phone number as a piece of information that does not relate to an identified or identifiable natural person. It is only through such a classification that one could rationally agree that the unintended disclosure or interception of the information would not give rise to a risk of negative consequence for the individual concerned.

90. It is unclear to me how one could reach such a conclusion in the context of the information in issue. As outlined above, the unique nature of a phone number is such that it inherently provides the means by which an individual can be identified. Thus, in the event that a mobile phone number is intercepted or otherwise disclosed between the point of its collection and the point in time at which it is lossy-hashed and irretrievably deleted, the intercepting party might well be able to identify the individual associated with that mobile phone number.

91. For the reasons set out above, my view is that, on balance, the mobile phone number of a non-user must be considered to be the personal data of the individual concerned. As regards the particular counter-arguments raised by WhatsApp in the Preliminary Draft Submissions, I have taken them into account, as part of my assessment, as follows:

The submission that inadequate account has been taken of the purpose of the processing, which is not aimed at the identification of non-users, but, rather, the aim of enabling WhatsApp to facilitate prompt and efficient connectivity for existing users when a new user joins the Service

92. While I accept that WhatsApp does not process the mobile phone numbers of non-users for the specific purpose of identifying those non-users, it is clear that the processing is designed to impact upon an individual non-user in the event that he/she subsequently decides to become a user of the Service. In other words, we are not dealing with separate "users" and "non-users"; rather, we are dealing with individuals who were originally "non-users" and have subsequently become "users". In this way, while the processing is not designed to *identify* the non-users concerned, it will, nonetheless, have individual and unique impact for the non-user concerned if he/she subsequently decides to become a user. In terms of that individual impact, it is clear that the processing is designed to make the individual's status, as a user, known to all of the other existing users who have the contact details of *this particular user* already stored in their devices. In other words, the prior activation of the Contact Feature, by any existing user whose address book contained the mobile phone number of the new user (at a time when that individual was a non-user), will result in that existing user learning that the new user has joined the Service by his/her automatic addition to the existing user's contact list within the app on his/her phone. In these circumstances, it is clear that the impact will be unique to each individual new user, given that each new user will have a different set of contacts. Thus, while the processing does not envisage the identification of the non-user, it is designed to have a particular and unique impact on each individual non-user, in the event that his/her non-user status changes in the future. In this way, it is arguable that, notwithstanding the lack of identification, the individual concerned has been 'singled out' (or will be singled out subsequently, i.e. upon becoming a user), as regards his/her treatment, pursuant to the processing.

93. I further note that, in having developed the Contact Feature as part of its product, WhatsApp has sought to ensure maximum convenience for its users. In effect, WhatsApp has chosen to develop the Contact Feature as part of its product and has done so on the basis that it will inevitably result in the processing of non-user data. While I accept WhatsApp's submissions that the Contact Feature benefits users, I do not accept that WhatsApp does not also derive a benefit; by ensuring maximum convenience for its users, WhatsApp ensures that its Service is attractive to potential new users who have a range of options to choose from, in terms of rival messaging services, thus harnessing the potential for ever greater numbers of new users signing up to the Service. Inevitably the more attractive / convenient a service is, the more users it will attract and, the more users a service has, the greater its commercial value to its owner. The processing of personal data involves risk for the data subjects concerned, hence the reason why the GDPR allocates significant responsibilities to

entities that process personal data. WhatsApp should not expect to be able to avoid those responsibilities, regardless of the limited scope of any such processing, particularly where it derives a benefit (direct or otherwise) therefrom.

The submission that, based on how WhatsApp's systems currently operate, it is not technically feasible for it to extract unhashed non-user numbers from the hashing process during the transient period it processes them. WhatsApp has further submitted, in this regard, that it would need to design and implement code changes in order to even access such non-user numbers

94. While I acknowledge WhatsApp's position that it has no desire to identify the non-users concerned, it is clear (from the analysis outlined above) that there are means available by which those non-users might be identified, both by WhatsApp and by third parties,. If it were the case that the absence of an intention to identify a data subject meant that the information in question could not constitute "personal data", then this would seriously undermine the breach reporting obligation in cases involving pseudonymised or incompletely-anonymised data. I further note, in this regard, that WhatsApp has the power to design and control the functionality of its own systems; while it has decided that it does not currently wish to identify non-users, there is nothing to prevent WhatsApp from changing its position on this. Further, it has the power to develop any required code and amend its terms and conditions of service to accommodate such a change of position. I am unable to attribute significant weight to these submissions in circumstances where circumventing any existing impediment to the identification of non-users is within the control of WhatsApp itself.

The submission that the Preliminary Draft does not take adequate account of the unique circumstances of the Breyer case

95. Insofar as I have referenced the *Breyer* case in the context of the pre-lossy hashing analysis, I do not agree that I am required to consider and put forward the specific circumstances in which WhatsApp might need or wish to refer a matter to An Garda Síochána for investigation. It is clear that An Garda Síochána is the competent Irish authority, as regards the investigation of criminal matters. It has a broad remit, in this regard. In the event that WhatsApp wished to report a matter of a criminal nature, including any possible incident of cybercrime, An Garda Síochána is the body to which such a report would be made. As part of any such reporting, An Garda Síochána would require WhatsApp to furnish all relevant information, including, where available, any associated mobile phone numbers. I further note, in this regard, that, while Recital 26 requires me to assess all of the "means reasonably likely to be used" to identify an individual, I am not required to assess the likelihood of whether or not the controller or a third party might *want* or *need* to avail of those means; once I am satisfied that there are means available that are reasonably likely to be used in the event that the controller or third party forms the intention to identify the individual concerned, that is the end of the matter. Support for this approach is to be found in the *Breyer* judgment where it is notable that the CJEU did not carry out any assessment of the likelihood of an event occurring, pursuant to which the controller might have grounds to support the making of contact with the competent authority such that the latter could take the steps necessary to obtain the additional information required to identify the data subject concerned from a third entity. I note that, in any event, my proposed finding does not substantially rely on the *Breyer* judgment, but, rather, the potential for identification inherent in the nature of a mobile phone number, as assessed by reference to Article 4(1) and Recital 26.

The submission that the proposed finding is not consistent with Recital 30 or the judgments of the CJEU in Lindqvist, Scarlet Extended or Nowak

96. I note that Recital 30 refers to the possibility that natural persons may be "associated with" online identifiers provided by their devices, such as IP addresses, and that "(t)his may leave traces which … may be used to create profiles of the natural persons and identify them". Recital 30 simply highlights the possibility that this type of association can lead to the identification of an individual because "traces" of the activities that have taken place through the operation of such online identifiers have enabled a profile to be created of the individual concerned such that he/she might be individually identified. Recital 30 does not operate to preclude the possibility that certain information, such as an IP address, might have the inherent possibility of identifying an individual. In any event, the information at issue is not an online identifier but a mobile phone number, which operates in an entirely different manner, in terms of providing a conduit to the individual concerned.

97. Further, while I accept that the circumstances of *Lindqvist*, *Scarlet Extended* and *Nowak* were such that the controller possessed both the information in issue as well as further identifying information, this does not preclude the possibility that certain information – such as a mobile phone number – might, in and of itself, enable the identification of an individual. I note, for example, that the CJEU's conclusion, in *Lindqvist*, was that "*the act of referring, on an internet page, to various persons* ***and identifying them by name or by other means, for instance by giving their telephone number*** *or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of [the Directive]*". [emphasis added]. This, in my view, leaves room for the possibility that an individual might be identified by way of a telephone number, even where – as here – this is the sole or main identifying factor. This is consistent with the Article 29 Working Party's Opinion 4/2007.

The submission that the proposed finding is not consistent with the principle of proportionality

98. WhatsApp has submitted, in this regard, that the momentary processing is undertaken "*solely for the purpose of enabling a hashing process that conclusively prevents any subsequent identification of the original mobile phone number (still less the owner of the number)*[44]". WhatsApp has further submitted that the transient processing does not have any meaningful privacy consequences for non-users. I note, in this regard, that the Article 29 Working Party considered proportionality in Section II of Opinion 4/2007, when it remarked that the Directive "contains a broad notion of personal data". It further observed that, while the "scope of the data protection rules should not be overstretched", "unduly restricting the interpretation of the concept of personal data should be avoided". Reflecting on the position further, the Article 29 Working Party suggested that the legislator had provided an indication as to how it wished the scope of the Directive to be applied, by way of the in-built exemptions, such as the previous exemption that applied where information was not part of a relevant filing system and the Recital 26 qualifier, that required the existence of a "means reasonably likely to be used … to identify the natural person".

99. The Article 29 Working Party observed that *"(i)t is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data … In fact, the text of the Directive invites to the development of a policy that combines a wide interpretation of the notion of personal data and an appropriate balance in the application of the Directive's rules*." It is, therefore, clear that I should not seek to restrict the interpretation of "personal data" but, rather, to consider proportionality in the context of the application of the rules set out in the GDPR to those data. This is the approach that I have taken

[44] The Preliminary Draft Submissions, paragraph 3.6

to the within assessment; I will consider the extent of the obligations arising pursuant to Articles 12 and 14 separately, below.

100. For the sake of completeness, I do not agree with WhatsApp's assertion that the processing which leads to the generation of the Lossy Hash does not have any meaningful privacy consequences for non-users. The right to exercise control over one's personal data is a key tenet of the GDPR. An individual might have made the deliberate choice not to become a user of the Service because he/she does not want WhatsApp, or any of its processors, to process his/her personal data. The Contact Feature completely disregards the non-user's right to exercise control over his/her personal data and instead places the responsibility on each individual user to either not use the Contact Feature or, in the alternative, to remove his/her non-user contacts from his/her address book. As such, WhatsApp has deliberately designed its system to this end.

101. Further, I do not think it reasonable to expect a user to remove a friend or contact from his/her address book – which is likely to also contain information that enables the user to communicate with his/her contacts through means other than the Service – in order to ensure that the personal data of a non-user contact is not processed by WhatsApp as a result of the activation of the Contact Feature. It is unclear, in any event, how an individual user might be expected to know which, of his/her contacts, are users of the Service and which are not. I note, in this regard, that WhatsApp has already acknowledged that an individual user will not be able to make this identification[45]. Lest it be suggested that non-users might inform their contacts of their status as a non-user, it is equally unclear how a non-user might be expected to know which, of the individuals that have his/her mobile phone number stored in their address book, are users of the Service.

102. Further, the fact that the Service currently operates in this manner – whereby the onus is on the individual user to either remove a contact from his/her address book or, in the alternative, avoid activating the Contact Feature – is likely to give rise to concern, on the part of non-users conscious of these issues, arising from the possibility that certain of their friends / contacts might have activated the Contact Feature, thereby enabling the processing of their personal data by WhatsApp.

103. Finally, and also of significance, as regards the purported transient or limited nature of the processing concerned, I note that, during the time that WhatsApp processes the information (up to the point of lossy hashing), it is subjected to the following operations:

    a. It is firstly **accessed** by WhatsApp;

    b. It is then **transferred** to WhatsApp's servers;

    c. The non-user number is then subjected to a lossy **hashing** process, following which;

    d. It is irretrievably **deleted**.

104. I note, in this regard, that Article 4(2) of the GDPR defines "processing" as meaning "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as **collection**, recording, organisation, structuring, storage, adaptation or

[45] The Inquiry Submissions, paragraph 4.7

alteration, retrieval, consultation, use, **disclosure by transmission**, dissemination or otherwise making available, alignment or combination, restriction, erasure or **destruction**" [emphasis added]. It is, therefore, clear that each of the four operations identified above are individually captured by the definition of "processing" set out in Article 4(2). I further note that the term "processing", as defined, is not subject to any temporal limits such that an operation that is performed on personal data for a very short period of time might be excluded from the definition set out in Article 4(2). Accordingly, I am satisfied that the operations performed on the information, by WhatsApp, constitute "processing", notwithstanding the short duration of the period of processing.

Finding: Does the phone number of a non-user, before the application of the lossy hashing process, constitute the personal data of that non-user?

105. Having taken account of WhatsApp's position, as communicated by way of the various submissions furnished during the course of the within inquiry, **I find that the mobile phone number of a non-user, before the application of the lossy hashing process, constitutes the personal data of that non-user**. As set out above, I have reached this conclusion on the basis that an individual is "identifiable" from his/her mobile phone number. This is so notwithstanding the limited and transient nature of the processing, in light of the ultimate consequence, for the non-user concerned, that flows from the processing. As observed above, the unique and individual impact of the processing upon each individual non-user crystallises at the point in time when that non-user becomes a user of the Service. At that point in time, any existing user who has previously activated the Contact Feature on their device and whose address book contained the mobile phone number of the new user (at a time when that individual was a non-user), will learn that the new user has joined the Service by his/her automatic addition to the existing user's contact list within the app on his/her phone.

Analysis and Discussion: Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?

106. Turning, then, to the status of a non-user's mobile phone number after the application of the lossy hashing process, I proposed a finding, in the Preliminary Draft, that this information also constituted the personal data of the non-user concerned.

107. WhatsApp, by way of the Preliminary Draft Submissions, provided new information, for the first time in the inquiry, which was described as "more technical detail[46]" as to the manner in which the Contact Feature operates. I note, in particular, that WhatsApp uses a Notification Hash, and not the Lossy Hash, at the notification stage in order to match up new users with existing users. I considered this new information to have been highly significant in the context of my assessment of this aspect of matters because it indicated that the lossy hashing process is not, in fact, the way in which WhatsApp achieves connectivity between new and existing users; rather, it operates merely as a filtering system to help reduce the number of devices to which WhatsApp will need to issue a Notification Hash when a new user joins the Service. In other words, the objective of the Contact Feature (i.e. connectivity between users) is achieved by the use of the Notification Hash, and not, as it previously appeared, by way of the Lossy Hash and Non-User List. I note that the Notification Hash is generated from the new user's mobile number only after the new user has joined the Service. In the circumstances, I proposed a finding, in the Composite Draft, that the phone number of a non-user, after the application of the lossy hashing process, does not constitute the personal data of that non-user. This is because the

[46] The Preliminary Draft Submissions, paragraph 3.2

phone number is irretrievably deleted immediately after the application of an irreversible lossy hashing process. The Lossy Hash generated, as explained above, is ambiguous in that it can represent any of at least sixteen mobile phone numbers. The result is that the information held by WhatsApp, in the form of the Lossy Hash, cannot be linked back to the non-user data subject concerned. While the Lossy Hash is stored in the Non-User List with the details of the associated user, it plays no further role in the process which results in the syncing of contacts, which is achieved through the use of a Notification Hash that is generated from the mobile phone number of the new user after he/she has joined the Service. That being the case, I did not need to engage further with the particular submissions made by WhatsApp concerning this aspect of matters (although I note that I have already engaged with most, if not all, of the particular submissions raised as part of my earlier assessment of the status of the non-user number prior to the application of the lossy hashing process).

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

108. The German (Federal), French, Portuguese, Hungarian, Dutch and Italian SAs each raised an objection to the finding proposed under this particular heading. The objections collectively identified various concerns in relation to the effectiveness of the lossy hashing process to achieve the anonymization of the underlying mobile phone number.

109. 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[47] as follows:

> *144. "For the purpose of assessing whether the data described above amounts to personal data, and also in consideration of WhatsApp IE's submissions in relation to the draft decision and the objections, the EDPB recalls the definition provided in Article 4(1) GDPR [48] and the clarifications provided by Recital 26 GDPR [49].*
>
> *145. In other words, WhatsApp IE needs to analyse whether data has been processed in such a way that it can no longer be used to directly or indirectly identify a natural person using "all the means likely reasonably to be used" by either the controller or a third party [50]. Such analysis needs to take account of objective factors as required by Recital 26 GDPR but can and should rely on hypotheticals allowing the understanding of the likelihood for re-identification to occur.*
>
> *146. In the case at hand, on the basis of the information available, the risk for non-users to be identifiable by inference, linking or singling out is not just "greater-than-zero"*

[47] The Article 65 Decision, paragraphs 144 to 156 (inclusive)

[48] Footnote from the Article 65 Decision: Article 4(1) GDPR: *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*.

[49] Footnote from the Article 65 Decision: Recital 26 GDPR: "*Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*".

[50] Footnote from the Article 65 Decision: WP29 Opinion 05/2014, page 5.

as acknowledged by the IE SA [51], but is such that it can be concluded that those non-users are identifiable for the purposes of the definition in Article 4(1) GDPR. The EDPB takes note of the statement by WhatsApp IE that "there is zero risk of re-identifying the original phone numbers from which they were generated" and "[e]ven if there was any re-identification risk, the factors applicable to the Anonymisation Process and creation of the Lossy Hash clearly demonstrate that any such risk has been reduced to below what the law sets as an acceptable risk level" [52]. However, the EDPB considers, as detailed below, that given the means and the data which are available to WhatsApp IE and are reasonably likely to be used, its capacity to single out data subjects is too high to consider the dataset anonymous.

147. The EDPB notes that, within its submissions, WhatsApp IE argued that the objections fail to identify why WhatsApp IE might want to single-out the non-users whose phone numbers have been deliberately subjected to a process that is designed to achieve anonymisation [53]. The EDPB highlights that neither the definition nor Recital 26 GDPR as such provide any indication that the intention nor the motivation of the controller or of the third party are relevant factors to be taken into consideration when assessing whether the dataset at hand is to be considered personal data or not [54]. The EDPB concurs with the IE SA, that what is relevant for the GDPR to apply, i.e. for data to be considered as "personal", is rather whether the data relate to a person who can be identified, directly or indirectly, and whether the controller or a third party have the technical ability to single out a data subject in a dataset [55]. This possibility may materialise irrespective of whether such technical ability is coupled with the motivation to re-identify or single out a data subject.

148. In addition, the EDPB stresses that the whole context of the processing needs to be considered, as "all objective factors" affect "whether means are reasonably likely to be used to identify the natural person" [56]. In the specific situation at hand, the creation of the Lossy Hashing procedure is only one step in the process and cannot be considered in isolation. Rather, the phone number of any user that activated the Contact Feature and that had at least at that moment one non-user contact will be linked to the lossy hash created from the number of this non-user [57]. The result is a "Non-User List" which is stored by WhatsApp IE [58].

149. As noted by the IE SA, viewing the hash value in isolation disregards the "risks present in the processing environment that might enable the re-identification of the data subjects concerned" [59]. Therefore, it is important to assess if the result of the entire process allows for singling out, rather than assessing an individual step of the process. For the possibility of re-identification, all the data and resources available to the controller or a third party needs to be considered. In this context, the EDPB does not consider that WhatsApp IE has conclusively shown that the processing environment is subject to such

[51] Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 56e.
[52] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 25.9.
[53] Footnote from the Article 65 Decision: WhatsApp LH Submissions, paragraphs 20 and 29.
[54] Footnote from the Article 65 Decision: See also WP29 Opinion 05/2014, page 10 ("for data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply.").
[55] Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 56.d.
[56] Footnote from the Article 65 Decision: Recital 26.
[57] Footnote from the Article 65 Decision: Draft Decision, paragraph 40.
[58] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 3.3 Step 3.
[59] Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 56.

organisational and technical measures that the risks of re-identification are purely speculative [60].

150. In its submission, WhatsApp IE indicates that each lossy hash represents a pool of at least 16 phone numbers [61]. However, in the view of the EDPB and as maintained by several objections raised by the CSAs, this is incorrect. While it cannot be ruled out that there will be cases where 16 phone numbers are connected to a lossy hash, in many cases a lossy hash will be connected to fewer phone numbers, even only one [62].

151. There is for example no certainty, nor is it likely, that all the theoretically available phone numbers in a range are indeed assigned to a data subject. Further, WhatsApp IE correctly points out in line with the NL SA's objection that the number of mobile phone numbers in the Netherlands exceeds the actual population. This leads to a situation where even though a lossy hash may refer to a set number of mobile phone numbers, the number of associated data subjects can be lower.

152. Additionally, considering that WhatsApp IE processes all the phone numbers that are contacts of the user that enables the Contact Feature, the EDPB notes that it is highly likely that a user will have at least one non-user phone number as a contact [63]. Therefore, the phone number of each user will be retrievable from the "Non-User lists" and these numbers can be used to exclude numbers that could be possibly represented in a lossy hash [64]. For example, if all but one phone number that would lead to a specific lossy hash are found to be users of the service, as they are part of at least one Non-User list, the remaining phone number is identified. Therefore, the proposed k-anonymity is not based on a k of 16 as indicated by WhatsApp IE, as that would require this value to be accurate for the entire data set.

153. For completeness, the EDPB refers to the Article 29 Working Party Opinion on anonymisation techniques [65], which clarified that k-anonymisation on its own merely avoids singling out, but does not necessarily address the risks of linkability or inference. In addition, it is to be noted that WhatsApp IE is even able to make use of the information on the devices of the users of its services, including the address book [66].

154. Further, the EDPB also notes that evidently the result of the Lossy Hashing procedure allows inferring information about a non-users or a set of non-users in relation to the phone number(s) to which the specific lossy hash correlates. For each of the user phone numbers in the Non-User list, it is provided that this user had at least one of the non-users' phone number, which is part of the set of non-user phone numbers represented by the lossy hash, in its address book when the user had activated that Contact Feature.

[60] Footnote from the Article 65 Decision: See WhatsApp Article 65 Submissions, paragraph 25.12.; WhatsApp LH Submissions, paragraph 12ff and 17ff.

[61] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 3.16.

[62] Footnote from the Article 65 Decision: For completeness sake, the 39bit kept allow for the representation of over 500 billion distinct values, which for all practical purposes should provide sufficient assurance that the appearance of collisions in practice is not significant.

[63] Footnote from the Article 65 Decision: This is particularly evident as the Contact Feature, according to the information provided by WhatsApp IE, does transfer any phone number, not only mobile phone numbers, and then applies the lossy hashing procedure to the non-user numbers.

[64] Footnote from the Article 65 Decision: See also PT SA Objection, paragraph 39.

[65] Footnote from the Article 65 Decision: WP29 Opinion 05/2014, page 24.

[66] Footnote from the Article 65 Decision: See also HU SA Objection, page 4, that re-identification may be achieved due to data in another database that the controller or other person may access.

> *155. Lastly, considering the amount of users of the service, the "Non-User List", which links each lossy hash and those users of the service that have at least one contact in their address book that would create this lossy hash, forms an extensive network of associations of users to various lossy hashes [67]. This network of connections between users and non-users, and thereby indirectly among users, constitutes a sort of topological signature of lossy hashes which becomes fairly unique as the dimension of the network and the number of connections grows [68]. This is the circumstance for the case at stake and the availability of the social graph among users and non-users can substantially increase the re-identification risk of data subjects [69].*
>
> *156. Therefore, based on the analysis done and the information available to it, the EDPB concludes that the table of lossy hashes together with the associated users' phone numbers as Non-User List constitutes personal data [70] and instructs the IE SA to amend its decision accordingly."*

Finding: Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?

110. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision **finds that the Non-User List comprising the table of lossy hashes together with the associated users' mobile phone numbers constitutes personal data**.

Relevant Background and Legal Analysis – Question (c)

Relevant Background

111. Having established that the data (i.e. the mobile phone number of each non-user contained in any existing user's address book) processed by WhatsApp constitutes the personal data of the non-users concerned, I am now required to determine whether WhatsApp processes that data as a data controller or, as WhatsApp asserts, as a data processor (acting on behalf of an individual user who has activated the Contact Feature).

112. Having assessed the information collected during the inquiry stage, I considered the following information to be relevant, for the purpose of this aspect of my assessment:

[67] Footnote from the Article 65 Decision: See also PT SA Objection, paragraph 42.

[68] Footnote from the Article 65 Decision: See for instance L Backstrom, C Dwork, J Kleinberg, *Wherefore art thou R3579X? Anonymized social networks, hidden patterns, and structural steganography*, Proceedings of the 16th international conference on World Wide Web, 181-190.

[69] Footnote from the Article 65 Decision: See NL SA Objection, paragraph 17 and 18 and FR SA Objection page 2. WhatsApp IE in its Submissions (WhatsApp LH Submissions) argues that it does not have a "social graph network" of the sort that appears envisaged by the objection, and that the service could be described as a "social graph network" only relating to the links between existing users of the service (and not non-users). However, the EDPB considers that the data provided in the Non-Users list is sufficient to allow for graph-based attacks, considering the means available to WhatsApp IE.

[70] Footnote from the Article 65 Decision: By this finding the EDPB also disagrees with WhatsApp IE's position in its Submission (WhatsApp LH Submissions, paragraph 14 and following), that the data is not pseudonymous but rather anonymous.

a. WhatsApp's Privacy Policy (as furnished during the course of the inquiry stage) includes reference to the processing of non-user data in the section entitled "Information We Collect", as follows:

> *"Information You Provide*
>
> - *Your Account Information. … You provide us, all in accordance with applicable laws, the phone numbers in your mobile address book on a regular basis, including those of both the users of our Services and your other contacts. …*
> *…*
> - *Your Connections. To help you organise how you communicate with others, we may help you identify your contacts who also use WhatsApp …"*

b. By way of an email to the Investigator dated 20 March 2019, WhatsApp clarified that EU users are invited to share their contacts with WhatsApp when registering for the Service and that *"(t)hey also have the ability to turn sharing of contacts on or off at any time after registration via their device settings*". A screen shot of the initial invitation was provided ("the **Contact Feature Pop-Up**") – that notification reads:

> *"WhatsApp" Would Like to Access Your Contacts*
>
> *Upload your contacts to WhatsApp's servers to help you quickly get in touch with your friends and help us provide a better experience"*
>
> *[Options provided]: "Don't Allow" or "OK"*

c. The information set out above appears to be the extent of the information that users are given in relation to the processing of non-user data that will take place upon activation of the Contact Feature.

Legal Analysis

113. To begin, it is useful to recall the definitions of "*controller*" and "*processor*", as set out in Articles 4(7) and 4(8) of the GDPR, as follows:

> *"'controller' means the natural or legal person … which, alone or jointly with others, determines the purposes and means of the processing of personal data …"*
>
> *"'processor' means a natural or legal person … which processes personal data on behalf of the controller"*

114. For the purpose of the within analysis, I will focus on the concept of controllership (in circumstances where WhatsApp is either a controller, for the purpose of any processing of non-user data, or it is not). I note, in this regard, that, while the definition of "*controller*" comprises a number of different elements, the key element for consideration is the identification of where the decision-making power lies, as between WhatsApp and an individual user. In other words: which party determines the "purposes and means" of the processing?

Opinion 1/2010

115. I note that the Article 29 Working Party considered the concepts of "*controller*" and "*processor*" in its Opinion 1/2010[71] ("**Opinion 1/2010**"). (Although updated guidelines[72] were published in September 2020, they post-dated the Preliminary Draft and Supplemental Draft such that they were not taken into account for the purpose of the analysis of the issues arising in this Part 1. In the circumstances, the Commission did not consider it appropriate to introduce reference to those updated guidelines for the first time in the Composite Draft and, accordingly, those updated guidelines are not referenced in this Decision). While Opinion 1/2010 considers these concepts by reference to the relevant definitions set out in the Directive, I note that those definitions mirror those set out in Articles 4(7) and 4(8) of the GDPR, above. As before, I am cognizant of the facts that (i) Opinion 1/2010 is non-binding; and (ii) the Article 29 Working Party was replaced, pursuant to Article 68 of the GDPR, by the European Data Protection Board on 25 May 2018. I consider, however, that the views expressed in Opinion 1/2010 nonetheless provide a helpful analysis of the factors that should be taken into account when considering whether a party is more properly classified as a "*controller*" or a "*processor*".

116. Considering the purpose and significance of the concept of controller, Opinion 1/2010 firstly observes that, in effect, "*all provisions setting conditions for lawful processing are essentially addressed to the controller, even if this is not always clearly expressed*." The basis for this observation appears to be the manner in which the rights of the data subject have been framed. Opinion 1/2010 notes, in this regard, that these rights:

> *"… have been framed in such a way as to create obligations for the controller. The controller is also central in the provisions on notification and prior checking … Finally, it should be no surprise that the controller is also held liable, in principle, for any damage resulting from unlawful processing … .*
>
> *This means that the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In order words: to allocate responsibility.*
>
> *This goes to the heart of the Directive, its first objective being "to protect individuals with regard to the processing of personal data". That objective can only be realised and made effective in practice, if those who are responsible for data processing can be sufficiently stimulated by legal and other means to take all the measures that are necessary to ensure that this protection is delivered in practice. This is confirmed in Article 17(1) of the Directive, according to which the controller "must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."*

117. Opinion 1/2010 further notes that:

> *"… the crucial challenge is thus to provide sufficient clarity to allow and ensure effective application and compliance in practice. In case of doubt, the solution that is most likely to promote such effects may well be the preferred option."*

[71] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted 16 February 2010 (00264/10/EN WP 169) ("**Opinion 1/2010**")
[72] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted 2 September 2020 (for public consultation)

118. Considering the factors that might be used to identify where the decision-making power lies, in terms of the determination of the "*purposes and means of the processing of personal data*", Opinion 1/2010 suggests that:

> "*one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions "why is this processing taking place? Who initiated it?"*
>
> *Being a controller is primarily the consequence of the factual circumstance than an entity has chosen to process personal data for its own purposes*."

119. Opinion 1/2010 further referenced *"(t)he need for a typology*", in this regard, observing that:

> *"The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. … However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. …*
>
> ***This calls for an interpretation of the Directive ensuring that the "determining body" can be easily and clearly identified in most situations, by reference to those – legal and/or factual – circumstances from which factual influence normally can be inferred, unless other elements indicate the contrary**."* [emphasis added]

120. Analysing what it means to determine "*the purposes and means of processing*", Opinion 1/2010 observes that this "*represents the substantive part of the test: what a party should determine in order to qualify as controller*". Opinion 1/2010 considers, in this regard, that:

> *"Determination of the "means" therefore includes both technical and organisational questions where the decision can be well delegated to processors (as e.g. "which hardware or software shall be used?") and essential elements which are traditionally and inherently reserved to the determination of the controller, such as "which data shall be processed?", "for how long shall they be processed?", "who shall have access to them?", and so on.*
>
> *Against this background, while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means.*
>
> *In this perspective, it is well possible that the technical and organisational means are determined exclusively by the data processor."*

121. Opinion 1/2010 concludes that:

> "*Determination of the "purpose" of processing is reserved to the "controller". Whoever makes this decision is therefore (de facto) controller. The determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned. Substantial questions which are essential to the core of lawfulness of processing are reserved to the controller. A person or entity who decides e.g. on how long data shall be stored or who shall have access to the data processed is acting as a 'controller' concerning this part of the use of data, and therefore has to comply with all controller's obligations."*

122. Summarising the above, it was the view of the Article 29 Working Party that:

a. The primary role of the concept of controller is to allocate responsibility. Responsibility, in this regard, means responsibility in the context of the protection of individuals with regard to the processing of personal data. In case of doubt, the solution that is most likely to promote such effects may well be the preferred option.

b. Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes.

c. When considering where the decision-making power lies, it is necessary to assess the specific processing operations and understand who determines them by firstly asking "why is this processing taking place? Who initiated it? Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes."

d. The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Determination of the purpose of the processing is reserved to the controller.

e. Determination of the "means" includes both technical and organisational questions where the decision can be delegated to the processor (e.g. "which hardware or software shall be used?"). Essential elements are traditionally and inherently reserved to the controller include determination as to "which data shall be processed?", "for how long shall they be processed?", "who shall have access to them", etc.

f. When considering the position, the need for a "typology" is important so as to ensure that the "determining body" can be easily and clearly identified in most situations by reference to circumstances from which factual influence can normally be inferred (unless other elements indicate to the contrary).

Relevant Caselaw

123. Noting the above, I now turn to two CJEU judgments in which the Court considered the allocation of responsibility in the context of relationships that comprised a natural person working in conjunction with a larger entity.

124. Turning, firstly, to the Facebook Fan Pages Case[73], the Court considered the processing of data in the context of a fan page that was hosted by Facebook but administered by a natural person. In that case, the Court noted the significance of the following factual realities;

a. Facebook placed cookies on the computer/device of persons visiting the fan page. This was the case regardless of whether or not the visitor was a Facebook account holder. These cookies, if not deleted, remained active for two years. In these circumstances, the Court considered that Facebook must be regarded as primarily determining the purposes and means of processing, in relation to the personal data of visitors to the fan page.

[73] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Case C-210/16, judgment delivered on 5 June 2018) ("the **Facebook Fan Pages Case**")

b. The Court further noted, however, that administrator of the fan page could obtain anonymous statistical information on visitors to the page via a function called "Facebook Insights". Facebook offered this function to the administrator, free of charge, pursuant to non-negotiable conditions of use. This function allowed the administrator to request such statistical information with the help of filters made available by Facebook. These filters enabled the administrator to define the criteria in accordance with which statistics would be collated by Facebook, including the ability to designate the categories of persons whose personal data would be processed, in this regard.

125. The Court noted that the objective of the controllership provision is to:

> *"ensure, through a broad definition of the concept of 'controller', effective and complete protection of the persons concerned". It noted that this concept "does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions."*

126. The Court observed that:

> *"While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account."*

127. The Court concluded that the fact that the administrator could, by way of the filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook, for this purpose, meant that the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.

128. The Court further noted that, while the audience statistics compiled by Facebook were transmitted to the fan page administrator in anonymised form, it remained the case that:

> *"the production of those statistics is based on the prior collection, by means of cookies installed by Facebook on the computers or other devices of visitors to that page, and the processing of the personal data of those visitors for such statistical purposes. The Court noted that "(i)n any event, [the Directive] does not, where several operators are jointly responsible for the same processing, require each of them to have access to the personal data concerned."*

129. The Court concluded that:

> *"In those circumstances, the administrator of a fan page hosted on Facebook … must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland."*

130. The Court added, however, that:

"the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."

131. Turning to the second case, the CJEU, in the Jehovah's Witnesses Case[74], had to determine the respective responsibilities of various parties in the context of personal data collected during the course of door-to-door preaching carried out by individual members of the Jehovah's Witness Community. In effect, the question for determination was whether "*a religious community may be regarded as a controller, jointly with its members who engage in preaching, with regard to the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community …*".

132. The Court had regard to the following factual background:

    a. The Jehovah's Witnesses Community organises, coordinates and encourages door-to-door preaching and, by way of its publications, has given guidelines on the collection of data in the course of that activity.

    b. The relevant supervisory authority previously found that the Jehovah's Witnesses Community had effective control over the means of data processing and the power to prohibit or limit that processing, and that it previously defined the purpose and means of data collection by giving guidelines on collection.

133. As before, the Court noted that the purpose of the concept of controllership is to:

    "ensure, through a broad definition of the concept of 'controller', effective and complete protection of the persons concerned, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the relevant case."

134. The Court further observed that:

    "a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller …"

135. Considering the position, the Court observed that:

    a. Individual members who engaged in preaching determined the specific circumstances in which they collected personal data concerning any persons visited, which specific data are collected, to that end, and how those data are subsequently processed;

[74] *Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta* (Case C-25/17, judgement delivered on 10 July 2018) ("the **Jehovah's Witnesses Case**")

b. The preaching activity itself, however, was organised, coordinated and encouraged by the Jehovah's Witnesses Community. In that context, the data in question were collected as a memory aid for later use and for a possible subsequent visit. The collection of personal data in this context was encouraged by the Jehovah's Witnesses Community.

c. The congregations of the Jehovah's Witnesses Community kept lists of persons who no longer wished to receive a visit. Those lists were compiled from the data that were transmitted to the congregations by individual members who engage in preaching.

136. The Court noted that, in the circumstances outlined above, the collection of personal data by individual members who engaged in preaching helped to achieve the objective of the Jehovah's Witnesses Community itself. Accordingly, it appeared to the Court that the Jehovah's Witnesses Community, by organising, coordinating and encouraging the preaching activities of its members intended to spread its faith, participated, jointly with its members who engage in preaching, in determining the purposes and means of processing of personal data of the persons contacted.

The Test to be Applied

137. The issue for determination is whether or not WhatsApp is a controller or a processor (acting on behalf of an individual user) when it processes the personal data of non-users pursuant to the activation of the Contact Feature.

138. I note the significance of the concept of controllership and the obligations that flow from that classification. I also note that the role of the concept of controllership is, first and foremost, to determine and allocate responsibility for compliance with data protection rules, including the exercise of rights by data subjects.

139. Allied with this is the need to ensure effectiveness, i.e. that any assessment of where the decision-making capacity lies should take account of predictability, with regard to control, as well as an outcome that ensures the effective protection of individuals' data protection rights. The outcome of the assessment should ensure "effective and complete protection" of data subjects. I note, in particular, that the CJEU has emphasised the connection between such comprehensive protection of data subjects and the correlative need to adopt a broad definition of the concept of controllership.

140. I agree that the status of controller is primarily a consequence of the factual circumstance that an entity has chosen to process personal data for his/her/its own purposes. I further note the importance of "the need for a typology", i.e. the importance of ensuring that the "determining body" can be easily and clearly identified in most situations by reference to those circumstances from which factual influence normally can be inferred, unless other elements indicate the contrary.

141. In terms of assessing where the decision-making ability lies in a multi-partite relationship, I note that the determination of the "purpose" of the processing is something that is solely reserved to the controller. The Article 29 Working Party noted that *"(w)hoever makes this decision is therefore (de facto) controller*". Similarly, questions which are essential to the core of lawfulness of processing are reserved to the controller. Such questions concern matters such as "*which data shall be processed?*", "*for how long shall they be stored?*" and "*who shall have access to them?*".

142. In relation to the determination of the "means" of processing, this aspect of matters includes questions that can be delegated to processors, such as decisions concerning technical and organisational issues (e.g. "*which hardware or software shall be used?*"). In this way, only decisions that concern the essential elements of the means of processing signify the required degree of control.

143. I further note, in the context of situations where the decision-making ability is shared between two different controllers, that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved. The CJEU has found that: *"(o)n the contrary, those operators may be involved at different stages of that process of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the relevant case"*.

144. I finally note that the classification of controller is not limited to corporate entities and that, as confirmed by the CJEU in the Jehovah's Witnesses Case, a natural person who "*exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller*".

145. Adopting the type of assessment recommended by the Article 29 Working Party in Opinion 1/2010 (as reflected by the CJEU in the Facebook Fan Pages and Jehovah's Witnesses Case), I note that the factual reality of the processing of non-user data in connection with the Contact Feature appears to be as follows:

a. What is the processing under assessment (by reference to any operations carried out on non-user personal data)?

The processing comprises five separate data processing operations: (i) the accessing, by WhatsApp, of the mobile phone numbers contained in an individual user's address book on a regular basis[75]; (ii) the transfer of those numbers to WhatsApp's servers[76]; (iii) the generation of irreversible hashes of the non-user numbers once they reach these servers[77]; (iv) the deletion of the underlying phone numbers[78]; and (v) the retention[79] of the Lossy Hash in the Non-User List on WhatsApp's servers, in conjunction with the details of the derivative user.

b. What is the purpose of the processing?

As established during the inquiry stage, non-user data is processed for two purposes:

I. It is firstly processed as WhatsApp tries to identify which, of the user's contacts, are already users of the Service (so as to update the user's WhatsApp contacts with those contacts that are also users of the Service)[80];

[75] Per the "Information We Collect" Section of the Privacy Policy
[76] The Preliminary Draft Submissions, paragraph 3.3
[77] Response to Investigator's Questions (response to question 3a.) and the Preliminary Draft Submissions, paragraph 3.3
[78] The Preliminary Draft Submissions, paragraph 3.3
[79] This arises as a consequence of the Board's determination of the lossy hashing objections, as detailed above, and as recorded at paragraph 156 of the Article 65 Decision.
[80] Response to Investigator's Questions (response to question 3a.)

II. It is secondly processed "*in order to quickly and conveniently update [a user's] contacts list on the Service as and when any of those non-users join the Service.*"[81]

c. Who decides which (non-user) data will be processed?

In order to be in a position to decide which data will be processed, the user must possess a certain level of knowledge about the purpose of the processing. The information provided to the user, however, by way of the Contact Feature Pop-Up, does not contain any reference to the purpose of the processing of non-user data, as identified above. I note, in fact, that the Contact Feature Pop-Up does not clearly identify, to the user, that (i) non-user data will be processed; and (ii) that it will be processed in the manner described at question a. above.

I further note that WhatsApp, in its Inquiry Submissions, explained that an opt-out (as had been suggested by the Investigator in her Draft Report) would be unworkable in circumstances where "*users generally have no way of knowing which of their contacts currently use the WhatsApp service prior to uploading their contacts, and so would have no way of knowing which friends' contact information they were opting-out from sharing*"[82]. If users have no way of identifying which of their contacts are currently users of the Service, it follows that they lack the knowledge required to be able to make decisions as to which (non-user) data will be processed.

Accordingly, it seems clear to me that WhatsApp decides which non-user data will be processed. In other words, it has designed its system so that all non-user data (insofar as the mobile phone number is concerned) will be processed where a user chooses to allow WhatsApp access to their address book contacts.

d. Who decides how long the data will be stored?

As already noted above, the Board has determined that the Lossy Hash, when stored in the Non-User List in conjunction with the details of the derivative user, constitutes personal data[83]. I note that neither the Privacy Policy nor the Contact Feature Pop-Up inform the user (i) that non-user data will be stored; and (ii) the period of time for which it will be stored. I cannot identify, from the information furnished by WhatsApp during the inquiry stage, the length of time for which the information is stored in the Non-User List on WhatsApp's servers. That being the case, it appears unlikely that a user would be able to identify this for himself/herself.

Accordingly, it again seems clear to me that WhatsApp decides how long the data will be stored.

e. Who decides who shall have access to the data?

The user decides to grant WhatsApp access to the data, while it is stored in the user's address book. As identified at question c. above, however, the information provided to the user, for the purpose of their deciding whether or not to grant access to their address book, does not identify that non-user data will be processed in the manner described at question a. That being the

[81] Response to Investigator's Questions (response to question 3a.)
[82] The Inquiry Submissions, paragraph 4.7
[83] The Article 65 Decision, paragraph 156

case, it is, in my view, unlikely that the user is even aware that their address book data will be transferred to WhatsApp's servers.

In the circumstances, it seems to me that, once the user has granted WhatsApp access to the address book on his/her device, the user has no ability to decide who has access to the data, after it has been transferred to WhatsApp's servers.

f. Who decides the means of processing?

As set out above, the user is not provided with sufficient information concerning the fact or purpose of processing of non-user data to allow him/her to understand the nature of the processing which WhatsApp will then undertake on that data. It follows that the user has no ability to make any decision concerning the means of processing.

g. Can the user exert influence over the processing of personal data, for his/her own purposes, and participate, as a result, in the determination of the purposes and means of that processing?

As set out above, the user is not informed, at any point in proceedings, that non-user data will be accessed and processed in the manner described above. In fact, the purpose of the processing, as identified at question b. above, is never disclosed to the user. In these circumstances, it is clear that the user does not have the ability to exert influence over the processing, for his/her own purposes, and participate, as a result, in the determination of the purposes and means of that processing. I do not consider that the fact that WhatsApp allows users a choice as to whether to grant access to their address book negatives the consequences I have identified here.

h. Can WhatsApp exert influence over the processing of personal data, for its own purposes, and participate, as a result, in the determination of the purposes and means of that processing?

It seems to me, from the above analysis, that WhatsApp is the only party that is in a position to exert influence over the processing of non-user data. While WhatsApp has asserted, throughout the within inquiry, that the processing is for the benefit of the user, it is clear, as I have set out earlier, that the processing of non-user data benefits WhatsApp. I note, in this regard, that the Contact Feature Pop-Up advises the user that the purpose of the Contact Feature is to "*help [the user] quickly get in touch with [his/her] friends*" and "*help [WhatsApp] provide a better experience*".

The Privacy Policy explains that: *"(t)o help [the user] organise how [he/she] communicate[s] with others, [WhatsApp] may help [the user] identify [his/her] contacts who also use WhatsApp*".[84]

On the basis of the above, it is clear that the processing of non-user data, as part of the Contact Feature, benefits WhatsApp in that it helps WhatsApp to "*provide a better experience*". It therefore seems to me that WhatsApp is in a position to exert influence over the processing of

[84] Per the "Information We Collect" section of the Privacy Policy

personal data, for its own purposes, and participate, as a result, in the determination of the purposes and means of that processing.

i. What is the "typology" here, i.e. what (legal and/or factual) circumstances are present from which factual influence could normally be inferred? What other elements are present to indicate the contrary?

I note that the Service is governed by terms of service that "*contractually mandate that WhatsApp is only for personal use*"[85]. I further note that the Service, in and of itself, along with any accompanying terms of service and user conditionality, were produced by WhatsApp. I note that an individual user cannot use the Service to communicate with the world at large; an individual user's ability to communicate is limited to his/her WhatsApp contacts. I further note that the Contact Feature has been designed by WhatsApp and that WhatsApp alone possesses the relevant knowledge in relation to how the Contact Feature operates in the context of non-user data. It is significant, in my view, that WhatsApp alone controls the information that is given to a user about the Contract Feature, its objective and how it operates. In this way, WhatsApp also controls the state of knowledge of the user, as regards the nature and manner of operation of the Contact Feature.

I further note that WhatsApp does not appear to make any attempt to inform the user that it regards the user to be the data controller, for the purpose of any processing operations carried out on non-user data (and indeed for the processing operations carried out on the personal data of other users that happen to be stored in the address book of the user's device) pursuant to activation of the Contact Feature.

Taking account of all of the factors outlined above, I am of the view that it would likely come as a surprise to a great many users of the Service to learn that WhatsApp considers them to be the data controller, for the purpose of non-user data processed as a result of activation of the Contact Feature.

In the circumstances, the "typology" is one of a private individual who uses a commercial messaging service, as a consumer, for purely personal communications. The individual's ability to communicate is limited to those other individuals that are users of the Service; the Service does not enable the user to communicate with non-users or the world at large. That being the case, the normal "typology", from a data protection perspective, is one where the service provider, being the party with the most significant decision-making power, is allocated the role of data controller. There do not appear to be any elements present, in the context of the Service under assessment, to indicate the contrary.

j. Are there any other factors that require consideration, in light of the need to ensure effectiveness and the requirement for a pragmatic approach that ensure predictability with regard to control?

It seems to me that there is no reality to WhatsApp's assertion that it is merely a processor when processing non-user data. As set out above, an individual user has no way of knowing, firstly,

[85] The Inquiry Submissions, paragraph 4.17(A)

that WhatsApp processes the data of any non-users that might be contained in the individual's address book. Further, as admitted by WhatsApp, an individual is not able to identify which, of his/her contacts, are users of the Service, even if he/she wished to assume the role of controller for the purpose of their personal data.

I further note that, even if WhatsApp's assertions were correct, and the individual user is the data controller of any non-user data, the relevant processing activities would likely fall outside of the scope of the GDPR by virtue of Article 2(2)(c), which provides that *"(t)his Regulation does not apply to the processing of personal data … by a natural person in the course of a purely personal or household activity*". Such a position would only serve to deprive a significant number of data subjects of the "*effective and complete protection*" described by the Article 29 Working Party in Opinion 1/2010.

The position is exacerbated, in my view, by the fact that a non-user, even though he/she might have actively chosen not to become a user of the Service, cannot avoid having his/her personal data processed by WhatsApp as a result of the activation of the Contact Feature by a user who happens to have the non-user's contact details stored on his/her device. The non-user has no say in matters whatsoever and the user, even if he/she were to be aware of the consequences of activating the Contact Feature, is equally powerless in circumstances where he/she has no way of knowing which of his/her contacts are users of the Service.

The fact that WhatsApp processes the personal data of non-users so as to be able to offer a better service to users denies the right of a non-user to decide that he/she does not wish his/her personal data to be processed by WhatsApp and disregards entirely the possibility that those non-users may never become users of the Service.

The Preliminary Draft and the Proposed Finding – Question (c)

146. By reference to the above analysis, I expressed the view, in the Preliminary Draft, that WhatsApp (and WhatsApp alone) appears to have made all of the decisions in relation to the core aspects of the processing of non-user data. Accordingly, I proposed a finding that, when processing non-user data, WhatsApp does so as a data controller, and not a processor.

WhatsApp's Response to the Proposed Finding – Question (c)

147. WhatsApp, by way of the Preliminary Draft Submissions, disagreed with my assessment and submitted[86] as follows:

    a. Purposes of Processing: "*The utility of the Service rests in substantial part on existing users being in a position to communicate readily with their contacts, including from the point that these contacts join WhatsApp as new users. The purpose of this processing is to enable existing users to quickly and efficiently keep their WhatsApp contacts up-to-date with other WhatsApp users who are in their device's address book. Users are free to use the contact Feature for this purpose or not. Users are also free to refuse permission for WhatsApp to access their mobile phone address book or withdraw any permission given at any time. WhatsApp would not be processing any such data for this purpose if it were not directed to by the user, and the user is*

[86] The Preliminary Draft Submission, paragraph 4.2

the one who benefits. The purpose of the processing is limited to the provision of the contact Feature and WhatsApp does not further process that data for any other purpose, in line with the fact that it does not have authority from the user to carry out any additional processing."

b. Which data will be processed: "*We consider it would be self-evident to users that they would grant WhatsApp permission to access their entire mobile phone address book – which by definition cannot be divided in advance into a WhatsApp user and non-user list – when asked to "Upload your contacts to WhatsApp's servers" in order to use the Contact Feature*."

c. Access to the data: "*Only WhatsApp (and its sub-processors) has access. Additionally, another layer of hashing and encryption is applied before storing non-user lossy hashes on the dedicated storage system and access to the storage system is restricted to WhatsApp's engineers and WhatsApp sub-processor personnel through access control rules*."

d. Means of processing: *"… it is the user that determines the "how" of the processing. … the functionality of the Contact Feature is such that the user determines which data will be processed (their contacts), for how long (until the user decides to delete any contacts or to de-activate the Contact Feature), and who shall have access (WhatsApp and its sub-processors). WhatsApp only determines the technical means of the processing*."

e. Influence over the processing: *"… it is the user that unilaterally determines if the processing takes place by enabling (or disabling) the Contact Feature for the purpose of helping the user "quickly get in touch with [their] friends". WhatsApp makes no such determination. If a user decides not to use the Contact Feature, withdraws permission for WhatsApp to access their contacts … , or if they delete a non-user contact from their address book, the processing does not happen*."

f. Typology: *"… a determination of whether a person is acting as a controller or processor must be assessed in the context of the specific processing at issue – rather than with the broad approach advocated by the Commission. In the specific context of the processing through the Contact Feature … it is the user, rather than WhatsApp who has the decision making power. The user determines the purpose and means of the processing of others' personal data through the Contact Feature. WhatsApp makes no such determinations and so cannot be allocated the role of controller in respect of the processing carried out through the Contact Feature*."

g. WhatsApp is processing for the user: "*By a user granting access to their contacts, WhatsApp suggests that it would be reasonable for a user to understand and assume that this entails a form of processing of all contacts (including non-users) by WhatsApp. While the Contact Feature doesn't allow the user to opt out certain contacts, the user still assumes the role of controller by making the decision that it wants WhatsApp to keep their WhatsApp contacts list up-to-date, and by determining the purposes and means of the processing …"*

h. Household exemption: *"… Recital 18 clearly envisages a scenario where a GDPR-regulated processor can act on behalf of a person that is not subject to the GDPR without that processor being deemed a controller. If the drafters of the GDPR had a concern about such a scenario arising and the impact on data subjects it could have legislated to provide that processors acting in such a capacity in those circumstances shall be treated as controllers – which it did*

not. Furthermore, purely from a practical perspective, the [Preliminary Draft] does not acknowledge that given the manner in which WhatsApp processes the data concerned (i.e. unhashed non-user numbers and lossy hashes) it would be impossible in any event for it to comply with any data subject requests, such as access and erasure. In light of this and WhatsApp's inability to identify and/or contact non-users, either when hashing their phone numbers … it is unclear what additional protection a non-user would benefit from by finding that WhatsApp is a controller."

i. Non-users: "*WhatsApp acknowledges that the operation of the Contact Feature is not technically possible for WhatsApp without the processing of all the contacts in a user's address book. However, a non-user is free to ask users to delete their number as a contact as they would be in any comparable context, such as storing details on phone or online communication or storage facilities. It is the user who decides whose numbers they store in their device address book; it is the user who decides they would like WhatsApp to keep their WhatsApp contacts list updated and determines the purposes and essential elements of the means of the process through the Contact Feature …"*

Analysis and Discussion: When processing the personal data of non-users, does WhatsApp do so as a data controller or a data processor?

148. I am not persuaded by the arguments raised by WhatsApp, as summarised above. I accept that the purpose of the processing is as outlined by WhatsApp. I do not, however, accept that the user is the sole beneficiary of the Contact Feature. WhatsApp has designed its product with maximum connectivity in mind. The Contact Feature ensures that a new user is able to communicate with contacts by way of the Service, immediately upon joining. Further, it ensures seamless growth of users' contact lists as more users sign up to use the Service. While this undoubtedly represents convenience for individual users, it also benefits WhatsApp by ensuring that its Service is attractive to potential new users who have a range of options to choose from, in terms of rival messaging services.

149. Further, while I accept that it is the user that determines whether or not to activate the Contact Feature, and that, once activated, the user is free to deactivate it at any time, this is not, in my view sufficient to outweigh the basic fact that it is WhatsApp, and WhatsApp alone, that designed the Contact Feature and controls its manner of operation. Further, WhatsApp, and WhatsApp alone, has the power to decide that the Contact Feature should be modified or updated and, again, it is WhatsApp alone that can implement any such changes by way of new code and/or amendments to the terms and conditions of service. In effect, the user is offered the binary choice of either using the Contact Feature or not; beyond this, the user has no ability to determine any aspect of the means and purposes of the processing. Additionally, and as noted in response to WhatsApp's submission that the purpose of the processing is not the identification of non-users, but rather to enable connectivity between users, I note that the new user has no ability to exercise control over the inclusion of his/her contact details in the WhatsApp contact list of any existing user who previously activated the Contact Feature and whose address book contained the mobile phone number of the non-user (at a time when that individual was a non-user). This occurs as a natural consequence of the Contact Feature, which itself relies on the prior processing of the non-user's number to create its effect.

150. I do not agree that it "would be self-evident to users" that, by activating the Contact Feature, WhatsApp will access and transmit all the numbers that might be stored therein to its servers. As

already noted, the user is provided with minimal information concerning the consequences of activating the Contact Feature. Further, it is unclear how the user might be expected to be in a position to determine the means and purposes of the processing when he/she is not in a position to know which of his/her contacts are already users of the Service such that he/she might understand the different impacts of the processing on his/her user and non-user contacts.

151. While I acknowledge that access to the data concerned might be limited (to WhatsApp and its "sub-processors"), the point is that the user has no ability to determine otherwise. As regards WhatsApp's submissions under the heading "typology", I do not agree with the suggestion that the above assessment represents a "broad approach", rather than an assessment "in the context of the specific processing at issue". The assessment outlined above has been carried out by reference to the specific processing operations, the specific features of the processing operations concerned and the specific impacts of same on non-users.

152. I agree with WhatsApp's submissions, as regards the interpretation of Recital 18 of the GDPR (the so-called 'household exemption'). It is appropriate, however, for me to note, as part of my overall assessment, the practical impact, from the perspective of the data subject, of a position whereby WhatsApp might be correct in its assertions that it is merely a processor for an existing user (who could, if designated the data controller, be subject to the exemptions from the controller obligations, as a result of the household exemption). Further, I do not agree with WhatsApp's submission that the manner in which it processes non-user data makes it impossible for it to comply with data subject requests. The right to information, for example, is one of the essential rights granted to data subjects pursuant to the GDPR. Even if a data controller is not in a position to provide a data subject with access to his/her data, it is still possible for that data controller to provide the data subject with the information prescribed by Articles 15(1) and (2).

153. Finally, and as already remarked upon earlier in this Decision, I do not think it reasonable to expect a user to remove a friend or contact from his/her address book in order to avoid the possibility of any non-user contact data being processed by WhatsApp upon the activation of the Contact Feature. An individual address book is likely to contain a variety of information concerning each contact, including landline telephone numbers and email addresses. Removing a contact from an address book, therefore, will inevitably result in significant inconvenience for both user and non-user concerned. Further, it is, in my view, somewhat glib to suggest that a non-user is "free to ask users to delete their number as a contact". The non-user, firstly, has no power to compel a user to honour such a request; further, as already observed, the removal of a contact will likely result in the deletion of all of the individual's contact details, and not just his/her mobile phone number, which would inevitably result in inconvenience to the user as regards communications with that individual. Further, it is unclear how the non-user might be expected to know which, of all of the individuals that might have his/her mobile phone number included in their address books, are users of the Service such that he/she might be expected to ask the user concerned to remove his/her details from their address book.

Finding: When processing the personal data of non-users, does WhatsApp do so as a data controller or a data processor?

154. For the reasons set out above, I remain of the view that WhatsApp (and WhatsApp alone) appears to have made all of the decisions in relation to the core aspects of the processing of non-user data. **Accordingly, I find that, when processing non-user data, WhatsApp does so as a data controller, and not a processor**.

Consequent Assessment of Compliance with the Requirements of Article 14

155. Having found that WhatsApp processes personal data relating to non-users and that, when doing so, it does so as a controller, the final issue for me to determine is the extent to which WhatsApp complies with the obligations set out in Articles 14 and 12(1) of the GDPR.

156. In the absence of any suggestion to the contrary, I noted, in the Preliminary Draft, that it appeared that WhatsApp has not provided any information to those non-users whose personal data has been processed pursuant to the Contact Feature. Accordingly, I proposed a finding that WhatsApp has failed to comply with its obligations to non-users pursuant to Article 14.

157. By way of the Preliminary Draft Submissions, WhatsApp submitted that "*(a)ny obligation … to comply with Article 14 GDPR has already been discharged in any event*". WhatsApp submitted, in this regard, that:

> "*In addition to the arguments regarding proportionality noted above, given that WhatsApp cannot contact these individuals directly, WhatsApp trusts the Commission would accept that Article 14(5)(b) GDPR would apply and that making information publicly available would be sufficient. As WhatsApp already makes information publicly available on the very limited way in which it engages with non-user data it is not clear what further information the Commission considers WhatsApp needs to provide in order to comply with Article 14(5)(b), should the Commission consider Article 14 GDPR to apply at all*[87]."

Analysis and Discussion: Article 14 Exemptions and Non-Users

158. I note that Article 14 provides a limited range of exemptions to the obligation to provide information to the data subject. These exemptions were considered in the Transparency Guidelines[88] (which, although prepared by the Article 29 Working Party, were subsequently adopted and endorsed on 25 May 2018 by the European Data Protection Board). The Article 29 Working Party firstly expressed the view that "(t)hese exceptions should, as a general rule, be interpreted and applied narrowly." In relation to Article 14(5)(b), the Article 29 Working Party considered that this allows for three separate situations where the obligation to provide the information specified by Article 14 is lifted, as follows:

    a. Where it proves impossible (in particular for archiving, scientific / historical research or statistical purposes);

    b. Where it would involve a disproportionate effort (in particular for archiving, scientific / historical research or statistical purposes); or

    c. Where providing the information required under Article 14(1) would make the achievement of the objectives of the processing impossible or seriously impair them.

159. WhatsApp has not identified which of the three situations it considers applicable. Neither has it furnished a sufficient explanation as to why it considers that situation to be applicable. The absence of such clarification (and supporting rationale) does not, however, prevent me from being able to

[87] The Preliminary Draft Submissions, paragraph 5.1

[88] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**") (see, in particular, paragraphs 57 – 65, inclusive)

reach a conclusion on this aspect of matters. This is because, even if the circumstances of the processing are such that WhatsApp is entitled to rely on the Article 14(5)(b) exemption, WhatsApp would still be required to "take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available." [emphasis added]

160. By way of its Article 65 Submissions[89], WhatsApp asserts that I must conclusively determine whether or not it is entitled to avail of the Article 14(5)(b) exemption in circumstances where such determination "would impact on the reasoning and the legitimacy of the findings" in this Decision. WhatsApp further submits that it would be "misplaced" for this Decision to find that it infringed the information obligations in Article 14 without establishing whether the main exemption to Article 14 applies. I do not agree with this assertion and remain of the view that such a determination is unnecessary in circumstances where WhatsApp has not made the prescribed information publicly available, as required by Article 14(5)(b). In effect, the Article 14(5)(b) exemption does not result in a situation whereby a data controller is free to ignore the obligations set out in Article 14; it merely permits the controller, where it satisfies the conditionality of Article 14(5)(b), to make the prescribed information publicly available, as opposed to providing it directly to the data subject concerned. Accordingly, the absence of a conclusive determination on the applicability or otherwise of the Article 14(5)(b) exemption does not have any, or any significant, impact on the outcome of the within inquiry (given my conclusion, as set out in paragraph 165 below, that WhatsApp does not currently make the required information publicly available).

161. I further note, in this regard, that WhatsApp does not consider that Article 14(5)(b) imposes an "absolute obligation" to make the transparency information publicly available "*in all cases, given the provision requires that the controller shall take "appropriate measures" (with making the information publicly available appearing as an example), and what is appropriate would fall to be assessed on the facts of a given case*[90]." To be absolutely clear about the position, the alternative condition, set out in Article 14(5)(b), requiring the controller to make the prescribed information publicly available is not optional or something to be assessed on a case by case basis; if a data controller is entitled to avail of the Article 14(5)(b) exemption, then it must make the prescribed information publicly available so that the data subjects concerned are nonetheless enabled to receive the Article 14 transparency information. This is clear not only from the text of Article 14(5)(b) but also from the limited nature of the exemptions provided by Article 14, which support the default position that the data subject must be provided with the prescribed information, save in very limited circumstances (which do not include those described by Article 14(5)(b)).

162. Notwithstanding the above, WhatsApp considers that it has complied with this requirement by making information publicly available "on the very limited way in which it engages with non-user data". It relies, in this regard, on the "public disclosure in the second paragraph of the Information We Collect section of the Privacy Policy" that states:

[89] The Article 65 Submissions, paragraphs 50 - 52
[90] The Article 65 Submissions, paragraph 51.15

"You provide us, all in accordance with applicable laws, the phone numbers in your mobile address book on a regular basis, including those of both the users of our Services and your other contacts. (emphasis added)[91]*"*

163. I firstly note that the above statement has been included in the Privacy Policy that is directed to users of the Service. It is unclear why a non-user of the Service would have reason to seek out this information by way of the Privacy Policy set out on WhatsApp's website. I secondly note that the information provided, by way of the above statement, is insufficient for the purpose of Article 14(5)(b). My view is that, in order to comply with the final sentence of Article 14(5)(b), the data controller concerned must make publicly available all of the information prescribed by Article 14. This is clear from the language of Article 14(5)(b) itself, which provides that:

> "*Paragraph 1 to 4 shall not apply where and insofar as … the provision of such information proves impossible or … In such cases, the controller shall take appropriate measures … including making the information publicly available*" [emphasis added]

164. The statement relied upon by WhatsApp does not provide the non-user data subject with all of the information that he/she is entitled to receive pursuant to Article 14. In particular, it does not inform the non-user of the consequences that will flow from the processing, in the event that he/she decides to sign up to become a user of the Service. This information is vitally important so as to enable the non-user to make an informed choice, in the event that he/she might consider joining the Service. The corresponding obligations arising in the context of Article 13 are assessed in Parts 2 and 3 of this Decision and the assessments and views expressed in those sections will help WhatsApp to understand what is required of it by Article 14, such that it might consider how to reformulate its approach to the delivery of the prescribed information to non-user data subjects.

165. Accordingly, I remain of the view that WhatsApp has failed to comply with its obligations pursuant to Article 14. As set out above, WhatsApp has failed to furnish the information required to enable me to understand why it considers Article 14(5)(b) to apply. Accordingly, I make no finding as to whether or not WhatsApp is entitled to rely on the Article 14(5)b) exemption (although I acknowledge, by reference to the consequences of a finding that WhatsApp might not be so entitled – as considered briefly below – that the circumstances of the processing are such that Article 14(5)(b) may well be applicable). My view, in this regard, is that, even if I were to find that WhatsApp is not entitled to rely on the Article 14(5)(b) exemption, it would not be appropriate, by reference to the manner in which WhatsApp currently processes non-user data, to require it to provide the Article 14 information to each non-user data subject individually. The practical impact of such an outcome would be a requirement for WhatsApp to subject non-user data to further processing operations, solely for the purpose of providing the information prescribed by Article 14 to each individual non-user data subject. Such a consequence would not respect the purpose limitation principle set out in Article 5(1)(b) and would not, in my view, serve the interests of the data subjects concerned.

166. As already observed, the unique and individual impact of the processing upon each individual non-user crystallises at the point in time when that non-user becomes a user of the Service. Accordingly, it is particularly important that WhatsApp clearly informs the non-user, as part of the sign-up process and prior to the conclusion of any contract between WhatsApp and the individual concerned, that (i) if his/her mobile phone number has been included in the address book of any of WhatsApp's existing

[91] The Preliminary Draft Submissions, footnote 51 (as referenced in paragraph 5.1)

users, and (ii) if any of those existing users activated the Contact Feature ("the **Activating Users**"), WhatsApp will have processed that mobile phone number for the purpose of quickly and conveniently updating those Activating Users' contacts lists on the Service as and when any of their non-user contacts join the Service; and that (iii) the practical consequence of this is that, if the individual joins the Service, his/her contact details will automatically appear in the WhatsApp contact lists of the Activating Users.

167. When considering its options, in terms of the formulation and delivery of the Article 14 information to non-user data subjects by way of a public notice, WhatsApp should give careful consideration to the location and placement of such a public notice so as to ensure that it is discovered and accessed by as wide an audience of non-users as possible. As noted above, a non-user is unlikely to have a reason to visit WhatsApp's website of his/her own volition such that he/she might discover the information which he/she is entitled to receive. Further, my view is that the non-user transparency information must be presented separately (by way of a separate notice, or a separate section within the existing Privacy Policy, or otherwise) to the user-facing transparency information so as to ensure that it is as easy as possible for non-users to discover and access the information that relates specifically to them. The information to be provided to non-users in compliance with Article 14 should, for the avoidance of doubt, detail the circumstances in which any non-user personal data is shared with any of the Facebook Companies, regardless of whether any such company is acting as a (joint) controller or a processor. In accordance with the direction of the Board[92], the information to be provided should further inform non-users about the retention of Lossy Hash values, in the Non-User List on WhatsApp's servers, in conjunction with the details of the derivative user(s).

Proportionality

168. As already noted, WhatsApp has submitted that:

> *"the application of the proportionality principle … leads to the conclusion that the processing of the unhashed mobile phone numbers by WhatsApp does not amount to the processing of personal data. The simple point is that the acutely transient nature of the processing, coupled with the facts that (a) the only data that is processed is the number and (b) the processing is undertaken merely as a precursor to a hashing process resulting in the irreversible anonymization of the number and designed to enable user-to-user connectivity (as opposed to the identification of non-users), leads to a result whereby it would not be proportionate to treat the processing as amounting to the processing of personal data. This is particularly the case given the lack of any meaningful privacy consequences for non-users[93]."*

169. I noted my view, above, that I should not seek to restrict the interpretation of "personal data" but, rather, to consider proportionality in the context of the application of the rules set out in the GDPR to those data. I further note that I have already explained why I do not agree with WhatsApp's submission concerning the "lack of any meaningful privacy consequences for non-users." Accordingly, I must now consider the question of whether the above assessment, concerning the application of the rules set out in Article 14 to the circumstances in which WhatsApp processes non-user data, is consistent with the principle of proportionality.

[92] The Article 65 Decision, paragraph 268
[93] The Preliminary Draft Submissions, paragraph 3.11

170. I firstly note, in this regard, that the principle of proportionality primarily operates to regulate the exercise of powers by the European Union. Pursuant to this principle, the action of the EU and any institutions / state organs within the EU, applying EU law, must be limited to what is necessary to achieve the objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued. The European Commission reflected the principle in its proposal of the new data protection framework (that would become the GDPR), as follows:

> "*The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal*[94]."

171. Further, when interpreting and applying EU law, the European Commission must not rely on an interpretation which would conflict with fundamental rights or with the other general principles of EU law, such as the principle of proportionality. In this regard, it is important to remember that the GDPR seeks to ensure the effective protection of the fundamental right to protection of one's personal data, as established by, and enshrined in, Article 8 of the Charter and Article 16 TFEU and Article 8 of the ECHR. The GDPR seeks to achieve this objective by way of:

    a. A set of core principles directed to ensuring that any processing of personal data is lawful, fair and transparent in relation to the data subject (and which are practically implemented by way of specific duties and obligations directed primarily to the data controller);

    b. A robust range of rights for the data subject, designed to empower the data subject to exercise control over his/her personal data and to hold the data controller accountable for compliance with the core principles; and

    c. The empowerment of supervisory authorities with a range of functions and powers, designed to enable those supervisory authorities to monitor and enforce compliance with the requirements of the framework.

172. In effect, the GDPR envisages a more active role for the data subject than ever before, with corresponding enhancements to the rights and entitlements that existed under the previous EU data protection framework. The effectiveness of those enhanced rights and entitlements, however, is entirely dependent on the data subject's state of knowledge. This was recognised by the CJEU in *Bara*[95], when the Court observed that:

> *"… the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed … and their right to object to the processing of those data …"*

173. It is noteworthy, in this regard, that the GDPR addresses the right to be informed by way of two separate provisions: Article 13, which governs the obligation to provide information in situations

[94] European Commission proposal (COM (2012) 11 final 2012/0011 (COD), published 25 January 2012

[95] *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF)* (Case C-201/14, judgment delivered by the CJEU on 1 October 2015) ("**Bara**")

where the information undergoing processing has been obtained directly from the data subject concerned, and Article 14, which governs the obligation to provide information in situations where the information undergoing processing has been obtained from a source other than the data subject. The fact that the legislator dedicated two separate provisions to the requirement for data controllers to provide information to data subjects is, in my view, very significant in that it indicates the importance of the right to be informed, in the context of the GDPR as a whole.

174. It is further noteworthy that the right to receive information is incorporated into other of the data subject rights, such as the right of access to personal data. In such a case, Articles 15(1) and (2) require the data controller to provide certain information to the data subject, as part of its response to the data subject concerned. It is therefore clear that the right to be informed is not only one of the core data subject rights, it is the bedrock upon which the other rights sit. It is only when the data subject has been provided with the information that he/she is entitled to receive, pursuant to Article 13/14, that he/she can understand (i) which of his/her personal data are being processed, (ii) for what processing operation(s), (iii) for what purpose(s), and (iv) in reliance on which legal basis. When the data subject has been provided with all of this information, he/she is afforded a sufficient state of knowledge such that he/she can meaningfully:

    a. exercise choice as to whether or not he/she might wish to exercise any of his/her data subject rights and, if so, which one(s);

    b. assess whether or not he/she satisfies any conditionality associated with the entitlement to exercise a particular right;

    c. assess whether or not he/she is entitled to have a particular right enforced by the data controller concerned; and

    d. assess whether or not he/she has a ground of complaint such as to be able to meaningfully assess whether or not he/she wishes to exercise his/her right to lodge a complaint with a supervisory authority.

175. I acknowledge that, in the context of the particular manner of processing of non-user data by WhatsApp, the rights that might be exercised by the non-user data subject concerned are limited. They are not, however, non-existent. While, for example, the non-user will not be able to be granted access to his/her personal data, WhatsApp could nonetheless provide him/her with the information prescribed by Articles 15(1) and (2). Further, the non-user can exercise his/her right to lodge a complaint with a supervisory authority. Further, there is a particular significance, of the right to receive information, for those non-users who might be considering joining the Service. The consequences of the processing, for that particular type of non-user arise when they enter into a contract with WhatsApp and become a user of the Service. The significance, of the right to receive information, in this particular context, is that it ensures that the non-user concerned is on notice of the consequences of the processing such that he/she can factor it into his/her decision as to whether or not he/she wishes to enter into a contract with WhatsApp to become a user. In this way, the information ensures that the non-user can make an informed choice as to whether or not he/she wishes to join the Service. It further ensures that the non-user is best positioned, if he/she decides to become a user, to provide informed consent to the processing of his/her personal data pursuant to any of the Service's voluntary features (such as the possible personalization of his/her user profile

to include a photograph). When all of these consequences are considered, it is clear that the right to receive information, even in the context of the limited processing envisaged by the Contact Feature, is inextricably connected with the right to exercise control over one's personal data.

176. Considering, then, the burden that the finding set out above might place on WhatsApp, I note that the non-user data undergoing processing is very limited, as are the processing operations that are applied to the data concerned. Accordingly, I do not consider that the preparation of the required information will be particularly burdensome for WhatsApp. My view is that the role and utility of the right to be informed, as considered above, outweighs the limited burden that would be placed on WhatsApp, as regards the formulation of the required information. In relation to the burden that would result from the requirement for WhatsApp to deliver that information to the data subjects concerned, I note that WhatsApp could, if it wished, deliver the required information by way of its existing policies and procedures. I note, in this regard, that WhatsApp could, as part of its existing onboarding procedure through the app, inform any non-user, who is considering joining the Service, of the consequences of the processing of non-user mobile phone numbers pursuant to the Contact Feature. Further, I note that WhatsApp's user-facing transparency information is already publicly available and, in the circumstances, the inclusion of the corresponding information required for non-users should not be a particularly burdensome or onerous task (and certainly not so burdensome that it would outweigh the data subjects' right to receive this information).

Finding: The extent to which WhatsApp complies with its obligations to non-users pursuant to Article 14 of the GDPR

177. **Accordingly, for the reasons set out above, I find that WhatsApp has failed to comply with its obligation to provide non-users with the information prescribed by Article 14.** For the avoidance of doubt, nothing in the above assessment should be interpreted as being an endorsement that the processing of non-user data, by WhatsApp, is conducted in reliance upon an appropriate legal basis. As already identified, the purpose of the within inquiry is to examine the extent to which WhatsApp complies with its transparency obligations pursuant to the GDPR and, in the circumstances, the assessment of the legal basis being relied upon to support any processing operation is outside of the scope of this inquiry.

Part 2: Transparency in the Context of Users

Introduction

178. Under this heading, I will consider the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of its processing of personal data relating to users of the Service. The issues that I will consider under this heading correspond to the matters covered by Conclusions 3 – 13 (inclusive) of the Final Report.

Relevant Provisions

179. Article 13 of the GDPR concerns transparency where the personal data in question "*are collected from the data subject*". In such a case, Article 13 requires the data subject to be provided with the following information:

    (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;

(g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(i) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(j) the right to lodge a complaint with a supervisory authority;

(k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(l) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

180. Article 12(1) complements this by requiring that:

"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing 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. … ."

181. Thus, while Article 13 addresses the information that must be communicated to the data subject, Article 12 addresses the *way* in which this information must be communicated.

Review of the Materials being relied upon by WhatsApp

182. In its Response to Investigator's Questions, WhatsApp advised that it provides users with the information prescribed by Article 13 of the GDPR "*via its Privacy Policy … and related pages (which are presented to users when they register to use the Service and are accessible at all times to users thereafter)*."

183. WhatsApp provided the Investigator with a copy of the privacy policy (the policy in question bearing a "last modified" date of 24 April 2018) ("the **Privacy Policy**") and "related pages" by way of Appendix 2 to its Response to Investigator's Questions. Appendix 2 was just over 16 pages in length (in the format furnished) and the content is set out by reference to the following main headings:

    a. WhatsApp Privacy Policy
    b. Information We Collect
    c. How We Use Information
    d. Information You And We Share
    e. How We Work With Other Facebook Companies
    f. Assignment, Change Of Control, And Transfer
    g. How The General Data Protection Regulation Applies To Our European Region Users
    h. Managing And Deleting Your Information
    i. Law And Protection
    j. Our Global Operations
    k. Updates To Our Policy
    l. Contact Information
    m. How We Process Your Information
    n. WhatsApp Inc., The EU-US Privacy Shield And The Swiss-US Privacy Shield
    o. Intellectual Property Policy: Your Copyrights And Trademarks
    p. Cookies

184. For the sake of completeness, I note that WhatsApp expressly referenced a further document in its Response to Investigator's Questions. In response to Question 4, WhatsApp confirmed that it "*identifies the purposes of processing personal data and the legal bases for such processing in the Privacy Policy and the 'How We Process Your Information' notice … "* [emphasis added]. WhatsApp provided the Investigator with a copy of this (undated) notice ("the **Legal Basis Notice**") by way of Appendix 4 to its Response to Investigator's Questions. This document, in the format furnished, was 4.5 pages in length.

Temporal Scope of this Assessment

185. For the avoidance of doubt, the assessments recorded in Parts 2 and 3 of this Decision reflect an assessment of the material relied upon by WhatsApp, **as available to the public at the date of commencement of the within inquiry (10 December 2018)**. I have not had regard to any amendments that might have been made to the material provided in the intervening time, save insofar as those amendments have rendered it unnecessary for me to issue a previously proposed direction to WhatsApp, as regards the remedial action required to address an identified issue that is not directly the subject of any finding (of infringement or otherwise).

How the User accesses and interacts with the Materials provided

186. Adopting the approach taken by the Investigator, I will firstly consider the contents of Appendix 2 and the Legal Basis Notice, both in the format furnished and in the online environment, so as to enable me to consider them from the perspective of the user.

Location and Accessibility of the Privacy Policy and the Legal Basis Notice: App Users

187. App users can access the Privacy Policy via the in-app "settings" options. Within the "settings" options, the Privacy Policy is clearly identified under the "Help" option. Within the "Help" option, the Privacy Policy is again clearly identified under the "Terms and Privacy Policy" option. Once selected, this brings the user to the "WhatsApp Legal Info" page on WhatsApp's website[96].

188. The "WhatsApp Legal Info" page provides app users with the following shortcut options:

    a. Key Updates [the linked notice is undated]
    b. Terms of Service [the linked document is identified as "Last modified: April 24, 2018"]
    c. Privacy Policy [the linked document is identified as "Last modified: April 24, 2018"]
    d. How We Process Your Information [the linked notice is undated]
    e. Privacy Shield [the linked notice is undated]
    f. IP Policy [the linked notice is undated]
    g. Cookies [the linked notice is undated]

189. The policies and notices listed above are presented in the form of a continuous scroll with one policy/notice running into the next, in the order set out above. For ease of reference, I will refer to this suite of documents as "the **Page**".

190. As observed by the Investigator, the shortcut options are set out at the top of the Page with the result that, when the reader scrolls down through the various polices/notices, the shortcut options are no longer visible. I note WhatsApp's submission, in this regard, that the reader can return to the top of the document by tapping "WhatsApp Legal Info" (which remains at the top of the page throughout). I agree, however, with the Investigator's view that this functionality is not immediately obvious to the user and, accordingly, I included a proposed direction, in the Preliminary Draft, requiring WhatsApp to take the action required to ensure that it is clear that the user can return to the top of the Page at any time by tapping "WhatsApp Legal Info". I note that WhatsApp has since taken the action required to address the substance of my concerns, in this regard, and, accordingly, the proposed direction is no longer required.

Location and Accessibility of the Privacy Policy and the Legal Basis Notice: Web Users

191. Web users can access the Privacy Policy by selecting "Privacy" from the list of options set out at the very end of WhatsApp's landing page[97]. The linked page contains a link to the Privacy Policy in the section entitled "Data transparency", located towards the end of the page. This link brings the user directly to the top of the Privacy Policy, as it is located within the scroll of policies and notices on the Page.

192. Like app users, web users are provided with a series of shortcut options, as follows:

    a. Key Updates [the linked notice is undated]

[96] www.whatsapp.com
[97] www.whatsapp.com

b. Terms of Service [the linked document is identified as "Last modified: April 24, 2018"]
c. Privacy Policy [the linked document is identified as "Last modified: April 24, 2018"]
d. How We Process Your Information [the linked notice is undated]
e. Privacy Shield [the linked notice is undated]
f. IP Policy [the linked notice is undated]
g. Cookies [the linked notice is undated]

193. Unlike app users, however, these shortcut options are located on the right of the Page and remain available to the user as he/she scrolls down the Page. In addition, web users are provided with a series of further shortcut options, in the form of an expanding list that appears when the user clicks on the Privacy Policy shortcut. The expanding list also appears automatically once the user reaches the Privacy Policy on the Page (i.e. the expanding list is presented to the user once he/she accesses the Privacy Policy, regardless of whether or not he/she has actively clicked on the Privacy Policy shortcut). The expanding list of additional shortcuts facilitate immediate access to the following specific sections of the Privacy Policy:

    a. Information We Collect
    b. How We Use Information
    c. Information You And We Share
    d. How We Work With Other Facebook Companies
    e. Assignment, Change of Control, And Transfer
    f. How The General Data Protection Regulation Applies To Our European Region Users
    g. Managing And Deleting Your Information
    h. Law And Protection
    i. Our Global Operations
    j. Updates To Our Policy
    k. Contact Information

194. As set out above, the Privacy Policy and Legal Basis Notice are two of a number of policy documents/notices available under the general heading of "WhatsApp Legal Info". The policy documents are not presented to the reader as separate documents; they are set out, one immediately following the other, in an unbroken scroll on the Page. As I will detail further below, the Privacy Policy and Legal Basis Notice incorporate reference (by way of a range of different hyperlinks embedded in the text of those documents) to most of the other documents/notices set out on the Page. For this reason, it was relevant for me to also consider the Privacy Policy and Legal Basis Notice from the perspective of their presentation to the user, as part of the Page, as well as the ways in which they interact with each other on the Page.

Presentation of, and Interaction between, the Privacy Policy and the Legal Basis Notice on the Page

195. I note that the Page, when copied into Word document format, runs to approximately 23 pages in length. The various documents and notices that make up the Page, their order of presentation and approximate length (when copied into Word document format, as before), are as follows:

    a. Key Updates (approximately 1 page in length - 4% of total Page length)
    b. Terms of Service (approximately 9 pages in length - 39% of total Page length)
    c. Privacy Policy (approximately 7 pages in length - 30% of total Page length)
    d. How We Process Your Information (approximately 3 pages long - 13% of total Page length)
    e. Privacy Shield (approximately 1 page in length - 4% of total Page length)

f. Intellectual Property Policy (approximately 1.5 pages in length - 7% of total Page length)
g. Cookies Policy (approximately 0.5 page in length - 2% of total Page length)

196. In terms of the interaction between the Privacy Policy and Legal Basis Notice, I firstly note that there is no reference whatsoever to the Legal Basis Notice within the Privacy Policy itself. This is surprising, given the significance of the information that the Legal Basis Notice purports to provide to the user. Further, the Privacy Policy only contains a single link to the Legal Basis Notice. This, too, is surprising in circumstances where the Privacy Policy appears to contain multiple links, spread throughout the document, to almost every other cross-referenced document/text. While that single link is contained in the "Our Legal Bases For Processing Information" sub-section of the section entitled "How The General Data Protection Regulation Applies To Our European Region Users", the link is embedded in in the text "Learn More". This is unfortunate given that this section contains a total of five links, the first three of which (embedded in the words "collect", "use" and "share") link the user back to earlier sections of the Privacy Policy, while the fourth one (embedded in the word "Terms") links the user to the Terms of Service with the last one being the "Learn More" link. There is nothing in this arrangement that would suggest, to the user, that the "Learn More" link will contain new and important information about WhatsApp's processing activities that he/she is entitled to receive.

197. In addition to this, I note that there is no reference whatsoever to the Legal Basis Notice at any point of the user engagement flow, regardless of whether the user engages with that flow as an app or web user. Consequently, a user wishing to access the prescribed information is provided directions by reference to the term "privacy policy" only; he/she has no way of knowing about the existence of the Legal Basis Notice, let alone that it contains some of the core information that he/she is entitled to receive pursuant to Article 13.

198. Turning, finally, to the format in which the Privacy Policy and Legal Basis Notice are presented to the user, I note that they are, respectively, the second and third documents in an overall scroll that comprises seven different policies/notices across a range of matters. Notwithstanding the availability of shortcut links, the Page, once accessed by the user, contains a significant amount of text (as documented above).

199. Considering this arrangement in the context of the obligations arising, Article 13 requires the data controller to "provide" the prescribed information to the data subject. Article 12(1) supports this by requiring the data controller to take "appropriate measures" to "provide" the information in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*".

200. In effect, Article 12(1) is directed to ensuring, insofar as possible, that the data subject *receives* the information that is "provided" by the data controller. It does this by reference to the potential barriers that could operate to prevent the information from being *received* by the data subject. The requirement, for example, for the data controller to use "clear and plain language" when "providing" the information helps to ensure that the data subject is not prevented from *receiving* the information because he/she could not understand complicated or technical jargon. Similarly, the requirement for the data controller to "provide" the information in a "concise" manner helps to ensure that the data subject is not prevented from *receiving* the information as a result of information fatigue caused by the incorporation of the information into a long and rambling piece of text.

201. Considering the format in which the Privacy Policy and Legal Basis Notice is presented to the user in light of the above, it is clear that, once a user reaches the Page, he/she is presented with a significant amount of text; this will be immediately apparent to the user, from the scroll bar running down the side of the Page. While the Privacy Policy and Legal Basis Notice only account for approximately 43% of the total text length, the user has no way of knowing this or of knowing, at first instance, whereabouts on the Page these are located. The use of this format to deliver the information prescribed by Article 13 of the GDPR risks dissuading the user from reading the Privacy Policy and Legal Basis Notice on the basis of a perception, on the part of the user, that he/she may be required to review a considerable length of text. In this way, the format of presentation risks creating a barrier between the prescribed information and the data subject.

202. Accordingly, and with a view to ensuring, insofar as possible, that users *receive* the information that WhatsApp is required to provide, I included proposed directions, in the Preliminary Draft, requiring WhatsApp to take action such that:

    a. the Legal Basis Notice is incorporated into (such that it forms part of) the Privacy Policy; and

    b. the Privacy Policy (with incorporated Legal Basis Notice) is separated from the remainder of the policies/notices that make up the Page and presented on a page of its own.

203. I note, however, that WhatsApp has since taken the action required to address the substance of my concerns, in this regard, and, accordingly, the proposed directions are no longer required.

204. For the avoidance of doubt, I note that the Investigator, by way of Conclusion 3, expressed the view that "*the format of the Online Documents in one continuous scrolling document is not in line with the accessibility requirement contained within Article 12.1 of the GDPR, as this scrolling [renders] specific information more difficult to find*." As detailed further below, I will approach the required assessment by reference to the individual categories of information that are prescribed by Article 13. Accordingly, I do not intend to propose any finding by reference to Conclusion 3 of the Final Report.

Methodology for Part 2: Assessment and Questions for Determination

205. Having established how WhatsApp provides information to its users, I must now consider the extent to which the measures implemented achieve compliance with the requirements of Article 13, read in conjunction with Article 12(1).

206. As set out above, Article 13 prescribes the information that must be provided to the data subject while Article 12(1) sets out the *way* in which this information should be provided. Thus, in order to achieve compliance with Article 13:

    a. The data controller must provide the required information; and

    b. Provide it in a manner that is "*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*"

207. In other words, compliance with Article 13 requires both of the above elements to be satisfied in each case.

208. Further, while the Investigator made findings by reference to WhatsApp's use of layering, I propose to approach the assessment strictly by reference to the requirements of Articles 12(1) and 13. Once the information has been provided (and) in a manner that complies with the requirements of Article 12(1), it matters not whether a data controller has achieved the objective by the use of layering or otherwise.

209. Finally, in terms of the limits of this assessment, my function is to assess the extent to which WhatsApp complies with its transparency obligations pursuant to Articles 12(1) and 13. This assessment does not permit or require me to inquire into, or otherwise, challenge the veracity of any information provided by WhatsApp to its users or to consider, for example, the appropriateness of any legal basis being relied upon to ground a particular processing operation.

210. Accordingly, the questions to be determined, by reference to each category of information prescribed by Articles 13(1) and 13(2), are:

    a. What information has been provided by WhatsApp? And

    b. How has that information been provided?

Approach to submissions furnished by WhatsApp at the Decision-Making Stage

211. WhatsApp furnished extensive submissions in response to the Preliminary Draft. Broadly speaking, those submissions can be divided into two categories:

    a. submissions directed to a specific aspect of Article 13 or a specific aspect of my assessment; and

    b. submissions concerning global matters, such that they are directed to an approach that I have taken generally or, otherwise, that have been directed to a number of the individual Article 13 assessments set out below ("**Submissions of General Application**").

212. In relation to the first category of submissions, I have recorded how I have taken account of the particular submissions made in the corresponding Article 13 assessment. In relation to the Submissions of General Application, however, I have, as a procedural economy and with a view to avoiding unnecessary duplication, recorded how I have taken these into account in this particular section of the Decision only. Thus, where, as part of its response to any of the individual assessments recorded in Parts 2 or 3 of this Decision, WhatsApp has included reference to any aspect of the Submissions of General Application, the views set out below can be taken to be the manner in which I have taken those submissions into account in the particular context.

Assessment of WhatsApp's Submissions of General Application

213. The Submissions of General Application can be grouped into four headings, as follows:

    a. Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related material;

    b. Submissions concerning Legal Certainty;

c. Submissions concerning Inconsistency; and

d. Submissions concerning WhatsApp's pre-GDPR engagement with the Commission.

214. The manner in which I have taken these four categories of submission into account, for the purpose of this Decision, is as follows:

Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related material

215. While WhatsApp maintains that it has complied with its obligations under the GDPR, it has confirmed that it is prepared to make, on a voluntary basis, amendments to its approach to transparency. It submitted, in this regard, that:

> *"While [WhatsApp] strongly maintains that it has complied with its obligations under the GDPR, WhatsApp has carefully reflected on the Commission's proposed findings, directions, views and obiter dicta comments in the [Preliminary Draft] and accepts that it can do more to improve the accessibility, quality and clarity of certain information it provides to users. WhatsApp intends to (i) take action to implement all of the Commission's proposed directions, and work is already underway to give effect to the directions requiring technical changes; and (ii) address most of the Commission's proposed findings and views by way of changes to the Privacy Policy and other user facing information. This workstream has already commenced as previously communicated to the Commission by WhatsApp. Parts C and D of [these Preliminary Draft Submissions] set out further details of the changes WhatsApp intends to make and the letter accompanying [these Preliminary Draft Submissions] addresses the timeframe in which these changes might be made, subject to the Commission's views[98]."*

216. WhatsApp identified the changes that it proposes to make, in this regard, throughout the Preliminary Draft Submissions[99]. Those changes include the implementation of the directions proposed in the Preliminary Draft, the improvement of the "educational information" that it provides to users in relation to the Contact Feature and the making of a range of other changes in response to the individual findings of infringement proposed by the Preliminary Draft.

217. WhatsApp stated that it hoped these commitments might help to "*convey how seriously it takes its transparency obligations and the level of thought, consideration and work that went into preparing the Privacy Policy and user facing information*[100]", such that I might reconsider my position on the findings proposed in the Preliminary Draft. While I acknowledge WhatsApp's willingness to amend its Privacy Policy and related material, this is not a matter that is relevant to the question of whether or not an infringement of the GDPR has occurred/is occurring in the context of the within inquiry. The assessments recorded in this Decision are based on the material relied upon by WhatsApp to achieve compliance with its transparency obligations as at the date of commencement of the within inquiry. This material forms the factual framework against which I have carried out my assessment. In the circumstances, I am unable to take account of any expressed willingness to change, on the part of WhatsApp, when determining, for the purpose of the within inquiry, whether or not an infringement

[98] The Preliminary Draft Submissions, paragraph 1.2

[99] See, in particular, paragraph 2.6(B), paragraph 2.6(D), paragraph 4.3, paragraph 6.2, paragraph 6.3, paragraph 6.7, paragraph 7.9, paragraph 7.11, paragraph 7.20, paragraph 7.21, paragraph 7.25, paragraph 8.4, paragraph 8.5, paragraph 9.5, paragraph 10.2, paragraph 11.3, paragraph 12.1, paragraph 14.4(B) and paragraph 14.10 of the Preliminary Draft Submissions

[100] The Preliminary Draft Submissions, paragraph 2.6(C)

of the GDPR has occurred/is occurring. I confirm, however, that I will take account of this aspect of matters in Part 5 of this Decision, as regards the question of the exercise of corrective powers, if any, that might be taken pursuant to any (concluded) finding of infringement which I might make.

Submissions concerning Legal Certainty

218. WhatsApp has submitted, in this regard, that:

> *"The principle of legal certainty dictates that organisations regulated by EU law are entitled to know and understand the standards to which they must adhere. In particular, WhatsApp considers that controllers should be able to have reference to the interpretations and standards set out in guidance issued or adopted by the [EDPB], such as the Transparency Guidelines, when deciding on an approach to compliance. In this regard, WhatsApp notes that its approach aligns with the approaches adopted by industry peers which reinforces WhatsApp's view that industry norms – based on good faith efforts to comply with GDPR – do not reflect the standards that the Commission is seeking to impose in the [Preliminary Draft]. Holding controllers to an alternative and even higher standard of compliance seems contrary to the function of the EDPB to promote and achieve through guidance a common and consistent application of the GDPR across the EU and results in a lack of legal certainty for controllers as to the nature and extent of their obligations[101]."*

219. WhatsApp has identified that these submissions have particular application in the context of my assessments of the obligations arising pursuant to Article 13(1)(c)[102] and Article 13(1)(f)[103]. WhatsApp further submits, in this regard, that:

> *"The Commission itself has not produced specific guidance detailing its expectations regarding compliance with the transparency requirements contained in the GDPR. Consequently this is the first time that WhatsApp has the benefit of the Commission's interpretation of many of these transparency requirements[104]."*

220. Having considered the above submissions, I firstly note that Articles 13 and 14 of the GDPR identify the particular information that data controllers must provide to data subjects. The language of these provisions is not technical or complex; each category of information is described in simple and clear terms. I further note that these provisions do not afford any discretion to the data controller, in relation to the prescribed information; unless the data controller is in a position to avail of one of the very limited exemptions provided, it must provide all of the information specified to the data subject. Article 12(1), as I have already observed, complements Articles 13 and 14 by identifying the way in which the specified information must be provided to the data subjects concerned. Article 12(1) affords the data controller discretion, in terms of the formulation and method of delivery of the specified information. This is a very limited discretion, however, given the express requirement for the information to be 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."

[101] The Preliminary Draft Submissions, paragraphs 2.1 and 2.3
[102] The Preliminary Draft Submissions, paragraphs 2.2, 6.6 and 6.18
[103] The Preliminary Draft Submissions, paragraph 9.4
[104] The Preliminary Draft Submissions, paragraph 2.2

221. The Article 29 Working Party sought to provide support to the data controller in the context of the transparency obligation. The resulting Transparency Guidelines[105] is a lengthy and comprehensive document that explores transparency from the perspectives of its utility and function, in the context of the GDPR. In this way, the data controller is enabled to understand the significance of the information that it has been tasked with providing such that it can ensure that it correctly formulates its approach to transparency. It is important to remember, in this regard, that there is no "one size fits all" approach to transparency; each data controller must formulate its approach to transparency by reference to its own particular data processing operations and the type of data subject concerned. In these circumstances, there is nothing further that the Commission could provide, by way of additional guidance, that has not already been covered by the Transparency Guidelines (or, indeed, by the GDPR itself).

222. As regards the suggestion that the approach I have taken in this Decision represents an "alternative" or "higher" standard of compliance, I fundamentally disagree with this. The GDPR requires the provision of certain, specified information to data subjects. In the context of any assessment of compliance, the data controller has either provided this information or it has not; there is no middle ground or room for the application of different standards. As regards the two particular aspects of my assessment – the approaches to Articles 13(1)(c) and 13(1)(f) – cited by WhatsApp in support of its submissions, I note that the approaches outlined in the Preliminary Draft match those outlined in the Transparency Guidelines, as follows:

    a. Under the heading "(c)lear and plain language", the Transparency Guidelines state that *"(t)he information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms of leave room for different interpretations. In particular the purposes of, and the legal basis for, processing the personal data should be clear"*[106] [emphasis added]. Thereafter follows a list of three "poor practice examples" and three "good practice examples". The explanations accompanying the "good practice examples" make it clear that, when providing information concerning the purpose of processing, the data controller must do so by identifying the "type(s) of data" that will be so processed. They further clearly identify that the information being provided should be linked to the "type(s) of data" undergoing processing. Accordingly, there is no difference whatsoever between the approach to Article 13(1)(c) outlined in the Preliminary Draft (i.e. the Proposed Approach) and the approach outlined by the Article 29 Working Party in the Transparency Guidelines.

    b. In relation to Article 13(1)(f), the Transparency Guidelines specifically state[107] that "*the information provided on transfers should be as meaningful as possible to data subjects; this will generally mean that the third countries be named."* It stands to reason that, in order for the information to be meaningful, the categories of data undergoing transfer must be provided to the data subject so that he/she can check that the transfer mechanism being relied upon permits the transfer of the category of data concerned.

[105] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")
[106] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 9
[107] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 38

223. Accordingly, I do not agree with any suggestion that a data controller is unable to know or understand the standards to which it must adhere, in the context of the transparency obligations. Neither do I agree that the absence of Commission guidance has left WhatsApp at a disadvantage, in terms of its ability to understand what is required of it pursuant to the transparency provisions. Further, I do not agree that the approaches outlined in the Preliminary Draft represent a higher (or alternative) standard of compliance to that required by the GDPR and/or the Transparency Guidelines.

224. Finally, I note WhatsApp's submission that its approach "*aligns with the approaches adopted by industry peers which reinforces WhatsApp's views that industry norms – based on good faith efforts to comply with GDPR – do not reflect the standards that the Commission is seeking to impose in the [Preliminary Draft]*[108]". If I were to take this submission into account, such that it might persuade me to reverse any proposed finding of non-compliance, it would be tantamount to saying that the standards of compliance required by the GDPR may be determined by the members of particular sectors of industry, rather than by the legislator. Such an approach is fundamentally incompatible with the GDPR; moreover, it would create a situation whereby individual data subjects would be afforded different standards of transparency depending on the particular industries with which they engage. For these reasons, I do not accept that this is a factor that I can take into account for the purposes of the assessments recorded in Parts 2 or 3 of this Decision.

Submissions concerning Inconsistency

225. WhatsApp has submitted, in this regard, that:

> *"WhatsApp is concerned that the manner in which the Commission has chosen to interpret the GDPR and the Transparency Guidelines … results in requirements that are inconsistent or are very challenging to implement in practice. By way of example as regards inconsistency, in respect of Article 13(1)(c) GDPR and WhatsApp's reliance on legitimate interests, the Commission, on the one hand, note that WhatsApp should adopt a "concise approach", and "user[s] should not have to work hard to access the prescribed information". However, on the other hand, in WhatsApp's view, the Commission's Proposed Approach in the Draft Decision would necessarily lead to information fatigue, and could actually make it harder and considerably more time consuming for users to understand the processing WhatsApp is carrying out. By way of further example, in respect of what WhatsApp considers to be the impractical nature of the Commission's interpretation, the Commission's requirement that WhatsApp identify the specific adequacy decision relied on in respect of each category of data could result in WhatsApp needing to continually update its Privacy Policy*[109]*."*

226. I do not share WhatsApp's concerns, in this regard. As is evident from the assessments that follow, my view is that the Privacy Policy and related material frequently demonstrate an over-supply of very high level, generalised information at the expense of a more concise and meaningful delivery of the essential information. Further, while WhatsApp has chosen to provide its transparency information by way of pieces of text, there are other options available, such as the possible incorporation of tables, which might enable WhatsApp to provide the information required in a clear and concise manner, particularly in the case of an information requirement comprising a number of linked elements. The importance of concision cannot be overstated, in this regard. For the avoidance of doubt, however,

[108] The Preliminary Draft Submissions, paragraph 2.3
[109] The Preliminary Draft Submissions, paragraph 2.5. See also paragraphs 6.9 and 6.14.

I am not saying that WhatsApp is not entitled to provide additional information to its users, above and beyond that required by Articles 13 and 14. WhatsApp is free to provide whatever additional information it wishes, providing that it has firstly complied with its statutory obligations and, secondly, that the additional information does not have the effect of creating information fatigue or otherwise diluting the effective delivery of the statutorily required information.

227. As regards the suggestion that a requirement for WhatsApp to identify the specific adequacy decision relied on in respect of each category of data could result in WhatsApp needing to continually update its Privacy Policy, I question how this might be the case. The categories of personal data being processed by WhatsApp are not extensive and, further, there are a limited number of adequacy decisions in existence. In any event, I do not agree that the burden that might be placed upon a data controller, in the context of a requirement for periodic updates to be made to its privacy policy, outweighs the right of the data subject to receive meaningful transparency information. The transparency obligation is an ongoing one, rather than one which can be complied with on a once-off basis, as with all controller obligations under the GDPR and inherent in this is the requirement that controllers continually monitor and review their practices to ensure continuing compliance with the GDPR. If it is the case that a data controller anticipates that it might have to update its privacy material from time to time, then it ought to take this into account when determining how it will formulate and deliver the prescribed information so as to make life as easy as possible for itself.

Submissions concerning WhatsApp's pre-GDPR engagement with the Commission

228. WhatsApp, by way of the Preliminary Draft Submissions, has also sought to partially defend its position, in a limited number of respects, by reference to its pre-GDPR engagement with the Commission. I note, for example, that, in relation to my comments concerning the placement of the Facebook FAQ and the fact that it is a stand-alone document (in the context of Part 3 of this Decision), WhatsApp has submitted that:

> *"The Facebook FAQ (as a stand-alone document) was first drafted on the basis of extensive consultation with the Commission. During that consultation the Commission did not take issue with the Facebook FAQ being provided as a stand-alone document. Nor has the Commission subsequently objected to maintaining the Facebook FAQ as a standalone document (on the understanding it is to be read in conjunction with the Privacy Policy which should refer to the Facebook FAQ). … [110]."*

229. It further submitted, in relation to my comments concerning the use of links to articles on Facebook's website, that:

> *"There is no requirement in the GDPR that prevents companies from referring individuals to information available from other sources and the Commission did not raise an issue with this approach previously[111].*

230. It is acknowledged that WhatsApp engaged in extensive consultation with the Commission's Consultation Unit in connection with the preparation of the Facebook FAQ. It is further acknowledged that the Commission's Consultation Unit has engaged (and continues to engage) with WhatsApp in relation to various matters, including transparency. I wish to make it very clear that, in the context

[110] The Preliminary Draft Submissions, paragraph 14.4(B)
[111] The Preliminary Draft Submissions, paragraph 14.10

of any such engagement, it is not the Commission's responsibility to carry out a detailed review of any material discussed or presented; neither is it appropriate for any data controller to expect the Commission to undertake any, or even partial, responsibility for ensuring that it is compliant with its obligations pursuant to the GDPR. As WhatsApp is aware, the function of the Commission's Consultation Unit is not to approve, or forensically examine, policy documents for a data controller or processor. Rather, it envisages a process of high level engagement with data controllers and processors in which the output, on the part of the Commission's Consultation Unit, is limited to the raising of questions or making of observations on the data protection aspects of the processing in issue. This approach reflects the accountability principle set out in Article 5(2) of the GDPR, which places the primary responsibility for compliance with the GDPR on the data controller or processor concerned.

231. For the sake of completeness, I note that WhatsApp has previously recognised that:

> *"During this period of [pre-GDPR] engagement, the DPC made it clear that it was not providing conclusive guidance on WhatsApp's proposed updates, and instead was providing an indication of issues which WhatsApp may have wished to consider while preparing its updates. We therefore acknowledge and understand that the feedback provided did not amount to approval of the approach WhatsApp was proposing[112]."*

232. In the circumstances, it is apparent that WhatsApp was clearly informed, at the relevant time, of the limited function and scope of any engagement with the Commission's consultation function. I therefore find it surprising that WhatsApp, having previously, in the course of this inquiry, openly acknowledged the limitations and true nature of the engagement with the Commission, would subsequently seek to recast that engagement and place reliance at the door of the Commission for decisions around transparency which are squarely the responsibility of WhatsApp

233. Having addressed the Submissions of General Application raised by WhatsApp, I will now proceed with my assessment of the extent to which WhatsApp has complied with the obligations arising by reference to the individual categories of information prescribed by Article 13. To the extent that WhatsApp might have included reference to any of the above matters of general application as part of its submissions in response to any individual category assessment set out below, the above reflects the manner in which I have taken those Submissions of General Application into account in the context of the particular category of information under assessment.

Assessment: Article 13(1)(a) – the identity and contact details of the controller

Required Information and WhatsApp's Response to Investigator's Questions

234. Article 13(1)(a) requires a data controller to provide the data subject with "*the identity and the contact details of the controller …* ".

235. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

[112] The Inquiry Submissions, paragraph 2.3

"The Privacy Policy identifies WhatsApp Ireland as the controller for users of the Service in the EU. Users can contact [WhatsApp] via a link provided in the Privacy Policy or alternatively using the details as provided in the 'Contact Information' section of the Privacy Policy."

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

236. The Investigator's views, in relation to the extent to which WhatsApp has complied with Article 13(1)(a), are set out by reference to Proposed Finding 4 of the Draft Report.

237. The Investigator proposed a finding that WhatsApp failed to clearly identify the data controller for the Service on the basis of inconsistencies between the language used in the Terms of Service and the language used in the Privacy Policy. Such inconsistencies, in the view of the Investigator, rendered the information provided "unclear and unintelligible", contrary to Article 12(1).

238. WhatsApp disagreed with the Investigator's assessment. It submitted[113] that the proposed finding ignored "the clear and unequivocal language in the Privacy Policy" and the fact that the Privacy Policy is the "primary information and transparency document in respect of WhatsApp's data processing".

239. The Investigator, however, was not swayed by WhatsApp's submissions and confirmed, by way of Conclusion 4, her view that the information provided by WhatsApp, in this regard, was "unclear and therefore contrary to Article 12(1) of the GDPR."

Assessment of Decision-Maker: What information has been provided?

Re: the requirement to provide the identity of the controller

240. The second paragraph of the Privacy Policy states that:

> *"If you live in a country in the European Economic Area (which includes the European Union), and any other included country or territory (collectively referred to as the European Region), your Services are provided by WhatsApp Ireland Limited ("WhatsApp Ireland"), which is also the data controller responsible for your information when you use our Services."*

Re: the requirement to provide the contact details of the controller

241. The "Contact Information" section of the Privacy Policy includes the following information:

> ***"If You Are In The European Region***
> *…*
> *If you have questions about our Privacy Policy, please contact us or write us here:*
> *WhatsApp Ireland Limited*
> *Attn: Privacy Policy*
> *4 Grand Canal Square*
> *Grand Canal Harbour*
> *Dublin 2*
> *Ireland"*

[113] The Inquiry Submissions, paragraphs 6.1 and 6.2

Assessment of Decision-Maker: How has the information been provided?

Re: the requirement to provide the identity of the controller

242. As set out above, the required information is set out at the beginning of the Privacy Policy.

243. I note that the Investigator expressed the view that the differences in the entities referenced, as between the Privacy Policy and the Terms of Service, gave rise to a risk of confusion in relation to the identity of the data controller for the Service. In this regard, and for the sake of completeness, I note that the "Key Updates" section (located at the very top of the Page) contains the following statement:

> *"**WhatsApp Ireland.** WhatsApp Ireland Limited provides our Services and is responsible for your information when you use WhatsApp."*

244. Further, the "Terms of Service" states that:

> *"**Our Services***
> *If you live in a country in the European Economic Area (which includes the European Union), and any other included country or territory (collectively referred to as the "European Region"), WhatsApp Ireland Limited provides the services described below to you; if you live in any other country except those in the European Region, it is WhatsApp Inc. (collectively, "WhatsApp," "our," "we," or "us") that provides the services described below to you (collectively, "Services"): …"*

Re: the requirement to provide the contact details of the controller

245. The contact details of the controller are clearly set out where they can be easily located (within the "Contact Information" section of the Privacy Policy).

Finding: Article 13(1)(a) – the identity and contact details of the controller

Re: the requirement to provide the identity of the controller

246. I do not share the Investigator's view that there is potential for confusion when identifying the data controller for the Service. The Privacy Policy, as submitted by WhatsApp, is clearly the primary source of information, for transparency purposes, and this document clearly identifies "WhatsApp Ireland Limited" as the relevant data controller. The position, as set out in the Terms of Service, is consistent with the information set out in the Privacy Policy.

247. Otherwise, the required information has been provided, in a clear way, at the outset of the Privacy Policy.

Re: the requirement to provide the contact details of the controller

248. This information has been provided, in a clear way, and in a location that might be expected to contain this information.

249. **Accordingly, I find that WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(a).**

Assessment: Article 13(1)(b) – the contact details of the data protection officer, where applicable

Required Information and WhatsApp's Response to Investigator's Questions

250. Article 13(1)(b) requires a data controller to provide the data subject with "*the contact details of the data protection officer, where applicable*".

251. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

> *"[WhatsApp] provides the contact details of its Data Protection Officer (DPO-inquiries@support.whatsapp.com) via a link in the 'Contact Information' section of the Privacy Policy."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

252. While the Investigator did not propose or confirm any particular finding or conclusion, under this heading, she confirmed, in the Draft Report and Final Report, that she was satisfied that WhatsApp had complied with its obligations pursuant to Article 13(1)(b).

Assessment of Decision-Maker: What information has been provided?

253. The "Contact Information" section of the Privacy Policy includes the following information:

> *"**If You Are In The European Region***
> *The Data Protection Officer for WhatsApp Ireland can be contacted here.*"*

Assessment of Decision-Maker: How has the information been provided?

254. The information has been included in the "Contact Information" section of the Privacy Policy. Once the link provided (as identified by an asterisk, above) is selected, it automatically generates an email, in a new window, addressed to DPO-inquiries@support.whatsapp.com. "WhatsApp Support – DPO" is auto populated into the subject line and the following text appears in the body of the email:

> *"Please edit this part to include the information below. Then, hit send. Thanks for contacting WhatsApp.*
>
> ** Your full name:*
> ** Your country of residence:*
> ** The phone number you used to create your WhatsApp account:*
> ** A detailed explanation of the issue you want to report to the DPO:"*

Finding: Article 13(1)(b) – the contact details of the data protection officer, where applicable

255. I note that the required information has been clearly set out, and has been made available to the user in a location in which this information might be expected to be found.

256. **Accordingly, I agree with the Investigator's conclusion and find that WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(b).**

Assessment: Article 13(1)(c) – the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

Required Information and WhatsApp's Response to Investigator's Questions

257. Article 13(1)(c) requires a data controller to provide the data subject with "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*."

258. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

> *"[WhatsApp] identifies the purposes of processing personal data and the legal bases for such processing in the Privacy Policy and the 'How We Process Your Information' notice …"*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

259. The Investigator set out her views on the extent to which WhatsApp complied with its obligations under this heading by reference to Proposed Findings 5, 6, 7 and 9.

260. By reference to **Proposed Finding 5**, the Investigator expressed the view that the information provided in the "Our Legal Bases for Processing Information" section of the Privacy Policy was insufficient to demonstrate WhatsApp's compliance with Article 13(1)(c) "as a first layer of information". In addition, the Investigator expressed the view that:

    a. The information provided by the data controller, pursuant to Article 13(1)(c), "should link the processing activity and the legal basis relied on by the data controller". The Investigator was of the view that this approach was consistent with the wording of Article 13(1)(c) and the views of the Working Party, as set out in the Transparency Guidelines.

    b. The Investigator was further of the view that the information should be provided by reference to a processing "operation" or "set of operations", in accordance with the definition of "processing" set out in Article 4(2) and the provisions of Recital 60.

261. WhatsApp disagreed with the Investigator's views, in this regard. It submitted that the GDPR does not require the precise legal bases being relied upon to be set out in the first layer of information[114]. WhatsApp further submitted[115] that the GDPR "does not require the separate disclosure of the legal basis for each and every processing operation."

262. The Investigator was unconvinced by WhatsApp's submissions and confirmed, firstly, that she remained of the view that references to "processing" should be understood as being references to a processing "operation" or "set of operations". By reference to that approach, the Investigator confirmed her view (by way of Conclusion 5) that the information provided under the sub-heading "Our Legal Bases for Processing Information" was insufficient to demonstrate WhatsApp's compliance with Article 13(1)(c) of the GPDR, as a first layer of information.

[114] The Inquiry Submissions, paragraph 7.3
[115] The Inquiry Submissions, paragraph 7.7

263. By reference to **Proposed Finding 6**, the Investigator set out her concerns in relation to the information that was provided to the user in relation to processing grounded on the contractual necessity basis (Article 6(1)(b)). She proposed a finding that "the disjointed manner in which the information is provided to data subjects regarding legal bases for processing of personal data, and the lack of clarity regarding the link between the purposes of processing and what the processing entails, is not in line with the requirements of Articles 12(1) and 13(1)(c) of the GDPR." The Investigator expressed the view, in this regard that:

> *"requiring a data subject to access four different locations from a second layer of information within a Privacy Policy, in order for that data subject to access all the requisite information to fully understand the purposes of the processing of their personal data, is not in line with the requirement set out in Article 12(1) of the GDPR for the information to be clear and intelligible."*

264. WhatsApp disagreed with the Investigator's views, in this regard. It submitted[116] that:

> *"Despite the assertions to the contrary in paragraph 162 of the Draft Report, users need only consult the "Our Services" section of the Terms of Service to understand the service provided under the contract. In reaching the view that users have to review the Terms of Service in their entirety, the [Investigator] has ignored the explicit statement in the "How We Process Your Information" notice that "We describe the contractual services for which this data processing is necessary in Our Services section of the Terms" (emphasis added)."*

265. WhatsApp further submitted[117] that "the "core data uses necessary to provide [the WhatsApp] contractual services" are specifically identified and listed in four bullet points in the contractual necessity section of the "How We Process Your Information" notice" and that "(t)hese four bullet points summarise in a clear and concise manner the processing that is necessary for the performance of the contract …".

266. The Investigator was unconvinced by WhatsApp's submissions, in this regard. She remained of the view that information concerning the purposes of processing and the legal basis for that processing should be linked in order for the provisions of Article 13(1)(c) to be satisfied. The Investigator concluded (by way of Conclusion 6) that the "disjointed manner in which the information is provided to data subjects regarding legal bases for processing of personal data, and the lack of clarity regarding the link between the purposes of processing and what that processing entails, is not in line with the requirements of Articles 12(1) and 13(1)(c) of the GDPR."

267. While the Investigator considered the section of the Legal Basis Notice that provided information concerning reliance on consent as a legal basis, she did not propose or confirm any particular finding or conclusion on this issue. She confirmed, however, that she was satisfied that the relevant section of the Legal Basis Notice was "sufficiently clear to comply with Article 13(1)(c) of the GDPR, albeit at the second layer of information, without the clear overview of the purposes of the processing, which [the Investigator believed] necessary at the first layer".

268. By reference to **Proposed Finding 7**, the Investigator set out her views in relation to the information that had been provided in relation to processing grounded on the legal obligations basis (Article

[116] The Inquiry Submissions, paragraph 8.4
[117] The Inquiry Submissions, paragraphs 8.5 and 8.6

6(1)(c)). The Investigator proposed a finding, under this heading, that WhatsApp failed to satisfy the requirements of Articles 12(1) and 13(1)(c) on the basis that:

a. The overview provided in the legal obligation section of the Legal Basis Notice, and the further information set out in the "Law And Protection" section of the Privacy Policy, did not provide the data subject with sufficient information about the extent to which WhatsApp relies upon this basis to ground the processing of personal data;

b. Further, the "broad and non-specific language utilised" in the "Law And Protection" section of the Privacy Policy did not provide clarity on the purposes for which any data are processed.

269. WhatsApp disagreed with the Investigator's views, submitting[118] that:

> *"… it is made clear to users that where law requires WhatsApp to process data in a certain way (for example, in response to a search warrant from An Garda Síochána), it relies on the legal obligation legal basis. Applying the correct legal standard, WhatsApp has both set out the purpose of processing (when the law requires it) and legal basis (compliance with a legal obligation), in this first sentence, as required by Article 13(1)(c)."*

270. WhatsApp further submitted[119] that:

> *"The "Law and Protection" section of the Privacy Policy … intentionally (and appropriately) describes processing which is broader than processing permitted on the basis of a legal obligation. For example, the "How We Process Your Information" notice also makes clear that WhatsApp relies on legitimate interests to "share information with others including law enforcement and to respond to legal requests" and this section of the fly-out also links to the "Law and Protection" part of the Privacy Policy. At no point does the "Law and Protection" section of the Privacy Policy purport to claim that WhatsApp only relies on a legal obligation to process personal data for these law and protection purposes.*
>
> *Finally, the Draft Report ignores the fact that, in light of the sensitive and often complicated processing that occurs in this area on the one hand, and the variety of legal reasons giving rise to a need to process personal data on the other, it is impossible to provide a full and fully nuanced descriptive account to users in respect of such processing without overloading them with information. For example, it would not be possible to provide further specificity in this section with regard to the multitude of circumstances in which WhatsApp will be required to assist law enforcement."*

271. The Investigator was unconvinced by WhatsApp's submissions, in this regard. She remained of the view that, as a result of the "broad and non-specific language utilised, the information provided in the "Law and Protection" section of the Privacy Policy leaves the user uncertain as to the circumstances in which WhatsApp will rely upon this legal basis for processing his/her personal data". The Investigator confirmed her view, by way of Conclusion 7, that WhatsApp was "not compliant with the requirements of Articles 12 and 13(1)(c) in relation to the information that it sets out pertaining to its legal basis for processing of personal data of compliance with a legal obligation."

[118] The Inquiry Submissions, paragraph 9.1
[119] The Inquiry Submissions, paragraphs 9.2 and 9.3

272. By reference to **Proposed Finding 9**, the Investigator set out her views in relation to the information that had been provided concerning WhatsApp's reliance on the legitimate interests ground. The Investigator expressed the view, in this regard, that the Article 13(1)(d) requirement to identify the legitimate interests being pursued was:

> *"a cumulative requirement, which results in Articles 13(1)(c) and 13(1)(d) operating together to place upon the data controller a requirement to set out the purposes of the processing in relation to the legitimate interests legal basis, along with the legitimate interests being pursued in carrying out the processing operations."*

273. The Investigator formed the view that the Legal Basis Notice "[conflated] the purposes of the processing of personal data with the legitimate interests relied upon to process personal data, without setting out any specific information in relation to the processing operation(s) or set of operations involved."

274. Accordingly, the Investigator proposed a finding that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

275. WhatsApp disagreed with the Investigator's views. It submitted[120] that:

> *"In assessing the adequacy of the information provided, the Draft Report also fails to take into account that the description of the purpose of the processing will often, in and of itself, necessarily identify the nature of the legitimate interest in issue. The proposed finding is also based on a mischaracterisation of the obligation on a controller under Article 13(1)(c) – i.e. there is no need to specify "processing operations" …."*

276. The Investigator was unconvinced by WhatsApp's submissions and confirmed her view, by way of Conclusion 9, that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

Preliminary Issue: What information must be provided pursuant to Article 13(1)(c)?

277. As set out above, there was substantial disagreement, as between WhatsApp and the Investigator, in relation to what information is required to be provided by Article 13(1)(c). In the Investigator's view, this provision requires a data controller to set out:

    a. "*A description of the purposes of processing;*

    b. *A description of the operation, or set of operations, underlying that purpose, undertaken by the data controller; and*

    c. *The legal basis relied upon by the data controller in order to carry out that processing operation, or set of operations*."

278. The Investigator was of the view that "*this information must be provided in such a manner so that the link between the operation (or set of operations), its purpose and the legal basis is clear*."

[120] The Inquiry Submissions, paragraph 11.1

279. WhatsApp disagreed with this and submitted that the Investigator sought to impose obligations on WhatsApp that go "above and beyond those prescribed by law". WhatsApp made this submission in relation to a number of the Investigator's proposed findings, including the proposed requirement for WhatsApp to:

> *"(B) link its legal bases for processing to specific processing operations, in addition to linking them to purposes for processing (which WhatsApp does), even though the GDPR only provides for the latter*[121] *… .*

280. WhatsApp expanded upon this submission by asserting[122] that Article 13(1)(c):

> "*does not require the separate disclosure of the legal basis for each and every processing operation. Indeed, while the term "processing operation" appears in a number of places in the GDPR, it is noticeably absent from the transparency obligations in Articles 12 through 14. Therefore, it is not understood why the Draft Report would purport to read such a requirement into Articles 13.1(c) and/or 13.1(d), especially given the prescriptive nature of Article 13. In addition, such a requirement is notably absent from the Transparency Guidelines which refer consistently to legal basis in the context of processing purposes, not processing operations. …"*

281. It thus appears that, while WhatsApp and the Investigator agree that Article 13(1)(c) requires a data controller to link the legal bases relied upon to the purposes of the processing concerned, they did not agree that, when providing this information, the controller must do so by reference to a specified "processing operation" or "set of operations".

Processing v Processing Operation

282. Article 4(2) provides that "(f)or the purposes of [the GDPR]":

> "'*processing' means* ***any operation or set of operations*** *which is performed on personal data or on sets of personal data, whether or not by automated means,* ***such as*** *collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*" [emphasis added]

283. Analysing the relevant elements of the above definition, I note that:

    a. "For the purposes of the GDPR" means that, each time the term "processing" is referenced in the GDPR, it should be understood to mean "processing", as defined by Article 4(2); and

    b. "Processing", by reference to Article 4(2), means "any operation or set of operations". While the GDPR does not contain a specific definition for an "operation", Article 4(2) identifies how this should be assessed, by reference to the list of examples that follow the words "such as". This list makes it clear that any action carried out on personal data, including its collection, is a processing "operation".

[121] The Inquiry Submissions, paragraph 1.6(B)
[122] The Inquiry Submissions, paragraph 7.7

284. I further note that this approach is consistent with Recital 60 (which acts as an aid to interpretation of Articles 12, 13 and 14), which provides that:

> "*The principles of fair and transparent processing require that the data subject be informed of the existence of* ***the processing operation*** *and its purposes. …*" [emphasis added]

285. This approach is also reflected in the Article 29 Working Party's Transparency Guidelines[123], which observe that:

> *"Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject. Connected to this, the accountability principle requires transparency of* ***processing operations*** *in order that data controllers are able to demonstrate compliance with their obligations under the GDPR."* [emphasis added]

286. As regards WhatsApp's submission that the absence of specific reference to processing "operation(s)" in Article 13 means that the obligation to provide information to data subjects does not necessitate an approach whereby the prescribed information is be provided by reference to individual processing operation(s), I am not persuaded by this argument. As set out above, Article 4 clearly identifies that the definitions set out in that article are "(f)or the purposes of" the GDPR. There is no limitation on the application of the prescribed definitions, either within Article 4 or in the context of individual provisions of the GDPR. That being the case, it seems to me that an argument premised on a suggestion that the definition of "processing" should only be applied to those provisions that incorporate specific reference, within its own text, to a processing "operation(s)", is unsustainable.

Analysis of Article 13(1)(c)

287. Applying the above to the provisions of Article 13, I note that Article 13(1)(c) requires the following:

> *"Where personal data … are* ***collected*** *from the data subject, the controller shall … provide the data subject with all of the following information:*
>
> *…*
>
> *(c) the purposes of the [processing operation]* ***for which the personal data are intended*** *as well as the legal basis for the [processing operation]"* [emphasis added]

288. While WhatsApp and the Investigator were agreed that Article 13(1)(c) requires a data controller to provide information in relation to the purpose(s) of the processing in conjunction with the corresponding legal basis for processing, it strikes me that the language highlighted in bold, above, suggests that the data controller should also provide this information in such a way that enables the data subject to understand which personal data are/will be processed, for what processing operation and by reference to which legal basis. In order to establish whether or not this is the correct approach, it is important to consider the role and function of Article 13 in the context of the GDPR as a whole.

289. Turning firstly to the core data protection principles, I note that Article 5(1) provides that:

[123] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")

"Personal data shall be:

(a) ***processed*** *lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

(b) ***collected for specified, explicit and legitimate purposes*** *and* ***not further processed in a manner that is incompatible with those purposes*** *… ('purpose limitation');*

(c) adequate, relevant and limited to what is ***necessary in relation to the purposes for which they are processed*** *('data minimisation');*

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to ***the purposes for which they are processed****, are erased or rectified without delay ('accuracy');*

(e) kept in a form which permits identification of data subjects for no longer than is necessary ***for the purposes for which the personal data are processed*** *… ('storage limitation');*

(f) ***processed*** *in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing … ('integrity and confidentiality')." [emphasis added]*

290. It can be observed, from the above, that there is a heavy focus, across the core principles, on the purpose(s) of the processing. It is further clear that, even though Article 5 describes six different principles, those principles are interconnected such that they operate, in combination, to underpin the data protection framework.

291. Considering, specifically, the purpose limitation principle, I note that this principle identifies the obligations arising by reference to the terms "collection" and "further" processing. This is very similar to the language of Article 13(1)(c) which contains separate references to "collection" and "the purposes of the processing for which the personal data are intended", i.e. it is couched in terms of "collection" and "further" processing. For this reason, it is useful to examine further the requirements and function of the purpose limitation principle enshrined in Article 5(1)(b) of the GDPR.

<u>The Article 29 Working Party's Opinion on Purpose Limitation</u>

292. The Article 29 Working Party considered the purpose limitation principle in its "Opinion 3/2013 on purpose limitation"[124] ("**Opinion 3/2013**"). As before, the Article 29 Working Party considered this issue in the context of the Directive however that consideration has equal application to the interpretation of the same principle in the context of the GDPR (given that the relevant text, in both the Directive and the GDPR, is materially identical). The Working Party observed that:

"*When setting out the requirement of compatibility, the Directive does not specifically refer to processing for the 'originally specified purposes' and processing for 'purposes defined subsequently'. Rather, it differentiates between the very first processing operation, which is*

[124] Article 29 Working Party, Opinion 3/2013 on purpose limitation, adopted 2 April 2013 (00569/13/EN WP 203) ("**Opinion 3/2013**")

collection, and all other subsequent processing operations (including for instance the very first typical processing operation following collection – the storage of data).

In other words: any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility."

293. The Working Party considered that the concept of purpose limitation comprises two main building blocks: 'purpose specification' and 'compatible use'. Considering the first of these building blocks, purpose specification, the Working Party noted as follows:

"*Article 6(1)(b) of the Directive requires that personal data should only be collected for 'specified, explicit and legitimate' purposes. Data are collected for certain aims; these aims are the 'raison d'être' of the processing operations.* ***As a prerequisite for other data quality requirements, purpose specification will determine the relevant data to be collected, retention periods, and all other key aspects of how personal data will be processed for the chosen purpose/s***." [emphasis added]

294. In relation to the significance of the purpose limitation principle and its relationship to other key elements of the data protection framework, the Working Party observed that:

"*There is a strong connection between transparency and purpose specification. When the specified purpose is visible and shared with stakeholders such as data protection authorities and data subjects, safeguards can be fully effective. Transparency ensures predictability and enables user control*."

295. Also:

"*In terms of accountability, specification of the purpose in writing and production of adequate documentation will help to demonstrate that the controller has complied with the requirement of Article 6(1)(b). It would allow data subjects to exercise their rights more effectively – for example, it would provide proof of the original purpose and allow comparison with subsequent processing purposes*."

296. In terms of the benefits for the data subject, the Working Party observed that:

"*In many situations, the requirement also allows data subjects to make informed choices – for example, to deal with a company that uses personal data for a limited set of purposes rather than with a company that uses personal data for a wider range of purposes*."

297. Further:

"*It should be kept in mind that processing of personal data has an impact on individuals' fundamental rights in terms of privacy and data protection. This impact on the rights of individuals must necessarily be accompanied by a limitation of the use that can be made of the data, and therefore by a limitation of purpose.* ***An erosion of the purpose limitation principle would consequently result in the erosion of all related data protection principles***." [emphasis added]

298. It is clear, from the above, that the purpose limitation principle has an important role to play, both in relation to the empowerment of the data subject but also in relation to underpinning and supporting the objectives of the data protection framework, as a whole.

299. It therefore seems to me that, when considering what information must be provided in relation to the "purposes" of any processing operation (such as by way of Article 13(1)(c)), I must do so by considering how the quality of information provided may potentially impact the effective operation of the other data protection principles. This is particularly the case where the wording of Article 13(1)(c) maps the approach of Article 5(1)(b), i.e. by describing the obligation arising by reference to "collection" and 'further' processing.

300. Given that the data controller identifies the categories of personal data that will need to be collected by the application of the purpose specification element of the purpose limitation principle, it seems to me that the provision of the Article 13(1)(c) information in conjunction with the category/categories of personal data being processed is essential if the data subject is to be empowered to hold the data controller accountable for compliance with the Article 5(1)(b) purpose limitation principle. The Article 29 Working Party reflects this approach in the Transparency Guidelines[125], as follows:

> *"Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles."*

Conclusion – Preliminary Issue: What information must be provided pursuant to Article 13(1)(c)?

301. By way of the Preliminary Draft, I set out my view that, in order to achieve compliance with the provisions of Article 13(1)(c), a data controller must provide the following information, and in the following way ("the **Proposed Approach**"):

    a. the purpose(s) of the specified processing operation/set of processing operations for which the (specified category/specified categories of) personal data are intended; and

    b. the legal basis being relied upon to support the processing operation/set of operations.

302. The information should be provided in such a way that there is a clear link from:

    a. a specified category/specified categories of personal data, to

    b. the purpose(s) of the specified processing operation/set of operations, and to

    c. the legal basis being relied upon to support that processing operation/set of operations.

303. The provision of the information in this manner is, in my view, consistent with language of Article 13(1)(c) and all of the elements that feed into, and flow from, the principle of transparency, including:

    a. the definition of "processing" set out in Article 4(2);

[125] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")

b. the Article 13(1)(c) requirement for a data controller to provide information in relation to "the purposes of the processing **for which the personal data are intended**" [emphasis added];

c. the role of the purpose limitation principle and the fact that the assessment required by this principle will determine what personal data will be collected for the particular purpose(s);

d. the fact that Article 5(1)(a) clearly envisages a user-centric approach, i.e. "(p)ersonal data shall be … processed lawfully, fairly and in a transparency manner in relation to the data subject" [emphasis added];

e. the role of transparency in the context of accountability; and

f. the requirement, set out in Article 5(2), for the controller to "be responsible for, and be able to demonstrate compliance with" all of the principles set out in Article 5(1), including the transparency and purpose limitation principles.

Proportionality and the Proposed Approach

304. Insofar as WhatsApp has submitted that the approach proposed by the Investigator, and incorporated into the Proposed Approach above, is inconsistent with the EU law principle of proportionality, I firstly note that this principle primarily operates to regulate the exercise of powers by the European Union. The principle[126] is enshrined in Article 5 of the Treaty on European Union, as follows:

> "*the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties*."

305. Pursuant to this rule, the action of the European Union (and any institutions / state organs within the EU, applying EU law) must be limited to what is necessary to achieve the objectives of the Treaties, i.e. the content and form of the action must be in keeping with the aim pursued. The European Commission confirmed that it took account of the principle when preparing its proposal in favour of the new data protection framework (that would become the GDPR)[127]:

> "*The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal."*

306. As I have referred to earlier in this Decision, when interpreting and applying EU law, the Commission must not rely on an interpretation which would be in conflict with fundamental rights or with the other general principles of EU law, such as the principle of proportionality. In this regard, I note that the GDPR seeks to ensure the effective protection of the fundamental right to protection of personal data as established by, and enshrined in, Article 8 of the Charter and Article 16 TFEU and Article 8 of the ECHR. The GDPR seeks to achieve this objective by way of:

[126] Article 52 of the Charter of Fundamental Rights of the EU also emphasises the requirement of proportionality, in relation to the application of rules concerning Charter protected rights.
[127] European Commission proposal (COM (2012) 11 final 2012/0011 (COD), published 25 January 2012

a. a set of core principles directed to ensuring that any processing of personal data is lawful, fair and transparent in relation to the data subject (and which are practically implemented by way of specific duties and obligations directed primarily to the data controller);

b. a robust range of rights for the data subject, designed to empower the data subject to exercise control over his/her personal data and to hold the data controller accountable for compliance with the core principles; and

c. the empowerment of supervisory authorities with a range of functions and powers, designed to enable those supervisory authorities to enforce compliance with the requirements of the framework.

307. As discussed briefly above, the GDPR envisages a more active role for the data subject than ever before, with corresponding enhancements to the rights and entitlements that existed under the previous framework. The effectiveness of those enhanced rights and entitlements, however, is entirely dependent on the data subject's state of knowledge. This fact was recognised by the CJEU in *Bara*[128], when the Court observed that:

> *"… the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed … and their right to object to the processing of those data …"*

308. The Proposed Approach represents, in my view, the minimum information required to give meaningful effect to the rights of the data subject. This approach respects the likelihood that:

a. a data controller will usually collect different categories of personal data from an individual data subject at different times, in different ways and for different purposes and a data subject may not always be aware that his/her personal data is being collected (because, for example, the data concerns the way in which a data subject interacts with a particular product or service and the data is collected by technology operating automatically as a component part of that product or service);

b. a data controller will always need to carry out more than one processing operation in order to achieve the stated purpose of a processing operation; and

c. a data controller might collect a particular category of data for a number of different purposes, each supported by a different legal basis.

309. Further, the Proposed Approach is, in my view, the only approach that will ensure, in each and every case, that a data subject has been provided with meaningful information such that he/she knows (i) which of his/her personal data are being processed, (ii) for what processing operation(s), (iii) for what purpose(s), and (iv) in reliance on which legal basis. It is only when the data subject has been provided with all of this information, that he/she is afforded a sufficient state of knowledge such that he/she can meaningfully:

[128] *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF)* (Case C-201/14, judgment delivered by the CJEU on 1 October 2015) ("**Bara**")

a. exercise choice as to whether or not he/she might wish to exercise any of his/her data subject rights and, if so, which one(s);

b. assess whether or not he/she satisfies any conditionality associated with the entitlement to exercise a particular right;

c. assess whether or not he/she is entitled to have a particular right enforced by the data controller concerned; and

d. assess whether or not he/she has a ground of complaint such as to be able to meaningfully assess whether or not he/she wishes to exercise his/her right to lodge a complaint with a supervisory authority.

310. In terms of assessing the corresponding burden on the data controller, I firstly note that a requirement for a data controller to provide the prescribed Article 13(1)(c) information in the manner required by the Proposed Approach does not require the controller to do anything that it is not already required to do. I note, in this regard:

a. The general principle of transparency set out in Article 5(1)(a) and detailed further in Articles 13 and 14;

b. The requirement, set out in Article 5(1)(b), for the data controller to carry out a purpose limitation assessment in order to determine, *inter alia*, the personal data that will need to be collected to satisfy the stated purpose(s); and

c. The requirement, pursuant to Article 5(2), for the data controller to be able to <u>demonstrate</u> compliance with all of the core principles.

311. Taking account of all of the above, it is my view that the Proposed Approach:

a. Requires the provision of the minimum information necessary to achieve the objectives of the GDPR; and

b. In doing so, does not place any additional obligation on the data controller.

312. Accordingly, the Preliminary Draft recorded my satisfaction that the Proposed Approach is consistent with the principle of proportionality.

<u>WhatsApp's Submissions in response to the Proposed Conclusion – Preliminary Issue:</u>

313. WhatsApp, by way of the Preliminary Draft Submissions, sought to challenge the Proposed Approach on a number of different grounds. WhatsApp firstly submitted that the Proposed Approach failed to "respect the clear choices made by the drafters of the GDPR[129]". It submitted, in this regard, that Article 13(1)(c) does not require the "categories of data" to be specified:

"It is significant that Article 13 GDPR is itself an extremely detailed and prescriptive provision. It is to be inferred in the circumstances that, had the legislators intended controllers to specify

[129] The Preliminary Draft Submissions, paragraph 6.5

the "categories of data" it was processing in the context of specific processing operations they would have made express provision for this. The fact that they have not done so reinforces against the imposition of this kind of granular obligation[130]."

314. It further submitted that:

"… it is clear from the fact that the concept is referred to in Article 14(1)(d) GDPR, that the legislators made a deliberate choice not to include this concept in Article 13(1)(c) GDPR. Moreover, if the Proposed Approach was correct there would be no need for Article 14(1)(d), as Article 14 GDPR would in any event have to be approached on the basis that categories of data needed to be identified. As such, the Proposed Approach appears to conflict with the statutory interpretation principle expressio unis est exclusion alterius [sic], it cannot be reconciled with the legislative intent of the drafters of the GDPR or the Transparency Guidelines including in particular the Annex to the Transparency Guidelines relating to "Information that must be provided to a data subject under Article 13 or Article 14[131]" …"

315. Having considered the above submissions, I note that the first fundamental difference between Article 13 and Article 14 is that Article 13 is expressly stated to apply in circumstances where "personal data are collected from the data subject". Article 14, on the other hand, only applies in circumstances where personal data have been obtained from a source(s) other than the data subject. The second fundamental difference is that the information prescribed by Article 13 must be provided to the data subject "at the time when personal data are obtained". The information prescribed by Article 14, however, can only be provided after the personal data has been collected.

316. These fundamental differences give rise to three variations, as between the information required to be provided pursuant to Article 13 and the information required to be provided pursuant to Article 14, as follows:

    a. Firstly, Article 13(2)(e) requires the controller to inform the data subject as to "*whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data*." Article 14, on the other hand, contains no such requirement. The rationale for this difference is clear: when this information is provided prior to the collection of personal data, the data subject is empowered to exercise control over his/her personal data because he/she is not placed in a position where he/she gives his/her personal data to the controller on a mistaken understanding as to the necessity for its collection and/or the potential consequences of failure to provide the data. The provision of such information would have no purpose if provided to the data subject *after* the personal data has been collected, hence its omission from Article 14.

    b. In relation to the second and third variations, Article 14(1)(d) requires the data subject to be provided with information as to the "categories of personal data concerned" while Article 14(2)(f) requires the provision of information as to the source "from which the personal data

[130] The Preliminary Draft Submissions, paragraph 6.11
[131] The Preliminary Draft Submissions, paragraph 6.12

originate". These requirements are notably absent from Article 13. In my view, the rationale for these omissions is clear, by reference to the exemption to the obligation to provide information set out in Article 13(4) and Article 14(5)(a). These exemptions provide that the controller's obligation to provide the specified information "shall not apply where and insofar as the data subject already has the information". In a case where the personal data has been collected from the data subject, there is no need to provide information as to the "categories of personal data concerned" or the source "from which the personal data originate" because the data subject already has this information; it is the data subject himself/herself that has provided the personal data to the controller and, in having done so, he/she already knows the "categories of personal data concerned" and the source. The data subject will not have this knowledge, however, if the data has been collected in the circumstances envisaged by Article 14. In my view, it is not the case that these two categories of information are only required to be provided pursuant to Article 14. Rather, both Article 13 and 14 envisage that this information will be provided but the circumstances in which Article 13 applies are such that the relevant information will already be known to the data subject concerned. In other words, Article 13 assumes that the data subject will already know the "categories of personal data concerned" and the source of the data.

317. Returning to the submissions made by WhatsApp under this particular heading, it is not the case that the Proposed Approach relies on an interpretation whereby the origin of the requirement to provide information detailing the particular categories of data is Article 13(1)(c) itself. Rather, my view is that Article 13 *presumes* that the data subject concerned already knows the "categories of personal data concerned" such that the purpose of Article 13(1)(c) is to inform the data subject about how that/those data will be processed by the controller and in reliance in which legal basis. To put it another way, my view is that Article 13 *presumes* that, aside from the information covered by Article 13(2)(e) (which, as noted above, serves no purpose once the personal data has been collected by the controller), a data subject should be no less informed if he/she is covered by Article 13 than he/she would be if he/she were to be covered by Article 14 (and vice versa). The analysis supporting the Proposed Approach, as already discussed, reflects this.

318. For the sake of completeness, I have also considered the position from the perspective advanced by WhatsApp, namely a position whereby Article 13 does not require the data subject to be informed as to the categories of personal data that the controller intends to be processed. It is unclear to me why a data subject would only be entitled to this information if the controller has acquired his/her personal data from another source. It is further difficult to understand how such a difference in treatment, between two categories of data subject, could be consistent with the GDPR, particularly where the difference in treatment concerns a core data subject right.

319. WhatsApp's Preliminary Draft Submissions secondly suggested that the Proposed Approach "cannot be reconciled with the wider requirements embodied in Article 12 GDPR.[132]" I have already considered these submissions as part of my assessment of WhatsApp's Submissions of General Application, at paragraphs 213 - 233, above.

[132] The Preliminary Draft Submissions, paragraphs 6.5, 6.9, 6.13 and 6.14

320. WhatsApp thirdly submitted that the Proposed Approach "*results in an approach that cannot be reconciled with the proportionality principle that governs the interpretation of this provision*[133]." It submitted, in this regard, that:

> *"The highly prescriptive notification provisions expressly embodied in Article 13 impose onerous burdens on controllers and, consistent with the proportionality principle, it is not possible to apply Article 13(1)(c) GDPR in the manner suggested by the Commission without arriving at a disproportionate result going beyond what is necessary to achieve the GDPR's objectives. Consequently, to the extent that Article 13(1)(c) GDPR is open to interpretation, it should be construed narrowly rather than the broad interpretation adopted by the Commission*[134]*."*

321. As is evident from the analysis of the Proposed Approach set out above, my assessment already takes account of the requirement for proportionality.

322. WhatsApp fourthly submitted that the rationale underpinning the Proposed Approach, namely the need to ensure that meaningful information is provided to empower data subjects to assess or exercise their rights and grounds for complaint, "*appears not to take into account the fact that WhatsApp does provide information on the categories of data it collects and processes to data subjects in the "Information We Collect" section of the Privacy Policy*.[135]"

323. WhatsApp is correct that, when formulating and assessing the Proposed Approach, I did not take account of the extent of information that WhatsApp provides to data subjects. This is because, when considering the issue, it was appropriate for me to do so in the abstract so as to identify the applicable requirements, against which I could assess the extent to which WhatsApp has complied with same. That assessment of compliance is set out below.

324. Having considered the various submissions made by WhatsApp, in relation to the Proposed Approach, **I maintain my view that the Proposed Approach correctly reflects the requirements of Article 13(1)(c).** That being the case, I will now proceed to assess the extent to which WhatsApp complies with its obligations pursuant to Article 13(1)(c).

Assessment: Application of the Proposed Approach to Article 13(1)(c)

325. As set out above, the information required to be provided by Article 13(1)(c), by reference to the Proposed Approach, is as follows:

    a. The purpose(s) of the specified processing operation/set of operations for which the specified category/categories of personal data are intended; and

    b. The legal basis being relied on to support the identified processing operation/set of operations.

326. As set out in its Response to Investigator's Questions, WhatsApp asserts that it provides the required information by way of the Privacy Policy and Legal Basis Notice. Turning firstly to the Privacy Policy, I note that the following information is provided under the heading "How The General Data Protection Regulation Applies To Our European Region Users":

[133] The Preliminary Draft Submissions, paragraph 6.5
[134] The Preliminary Draft Submissions, paragraph 6.17
[135] The Preliminary Draft Submissions, paragraph 6.15

> *"We collect, use, and share the information we have as described above:*
> - *as necessary to fulfill our Terms;*
> - *consistent with your consent, which you can revoke at any time;*
> - *as necessary to comply with our legal obligations;*
> - *occasionally to protect your vital interests, or those of others;*
> - *as necessary in the public interest; and*
> - *as necessary for our (or others') legitimate interests, including our interests in providing an innovative, relevant, safe, and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data. Learn More"*

327. Once the link embedded in the text "Learn More" is selected, the user is brought to the Legal Basis Notice where further information is provided in relation to the identified legal bases.

328. For ease of review, I will proceed with my assessment of the extent to which WhatsApp complies with its obligations pursuant to Article 13(1)(c) by reference to the individual legal bases identified by WhatsApp in the Privacy Policy (and elaborated upon in the Legal Basis Notice). I will set out my views under the heading "assessment" at the end of every section however, for the avoidance of doubt, I will only make a single finding in relation to the extent to which WhatsApp complies with its obligations under Article 13(1)(c), read in conjunction with Article 12(1).

Identified Legal Basis 1: Contractual Necessity

What information has been provided?

329. In this section, I will examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(b) (referred to as "contractual necessity"). The Legal Basis Notice provides, in this regard, that:

> *"For all people who have legal capacity to enter into an enforceable contract, we process data as necessary to perform our contracts with you (the Terms of Service, the "Terms"). We describe the contractual services for which this data processing is necessary in Our Services section of the Terms and in the additional informational resources accessible from our Terms. The core data uses necessary to provide our contractual services are:*
>
> - *To provide, improve, customize, and support our Services as described in "Our Services";*
> - *To promote safety and security;*
> - *To transfer, transmit, store, or process your data outside the EEA, including to within the United States and other countries; and*
> - *To communicate with you, for example, on Service-related issues.*
>
> *These uses are explained in more detail in our Privacy Policy, under How We Use Information and Our Global Operations. We'll use the data we have to provide these services; if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted."*

330. As is clear from the above, the user is invited to receive more information by reference to the links embedded in the following text:

a. "Terms of Service" – this links the user to the top of the Terms of Service, on the Page. As set out above, this is a relatively lengthy document (that contains further links to other documents, including the Privacy Policy itself).

b. "Our Service" – this links the user to the section entitled "Our Service" within the Terms of Service. The information available here is as follows:

- *"**Privacy And Security Principles.** Since we started WhatsApp, we've built our Services with strong privacy and security principles in mind.*
- ***Connecting You With Other People.** We provide ways for you to communicate with other WhatsApp users including through messages, voice and video calls, sending images and video, showing your status, and sharing your location with others when you choose. We may provide a convenient platform that enables you to send and receive money to or from other users across our platform. WhatsApp works with partners, service providers, and affiliated companies to help us provide ways for you to connect with their services. We use the information we receive from them to help operate, provide, and improve our Services.*
- ***Ways To Improve Our Services.** We analyze how you make use of WhatsApp, in order to improve all aspects of our Services described here, including helping businesses who use WhatsApp measure the effectiveness and distribution of their services and messages. WhatsApp uses the information it has and also works with partners, service providers, and affiliated companies to do this.*
- ***Communicating With Businesses.** We provide ways for you and third parties, like businesses, to communicate with each other using WhatsApp, such as through order, transaction, and appointment information, delivery and shipping notifications, product and service updates, and marketing. Messages you may receive containing marketing could include an offer for something that might interest you. We do not want you to have a spammy experience; as with all of your messages, you can manage these communications, and we will honor the choices you make.*
- ***Safety And Security.** We work to protect the safety and security of WhatsApp by appropriately dealing with abusive people and activity and violations of our Terms. We prohibit misuse of our Services, harmful conduct towards others, and violations of our Terms and policies, and address situations where we may be able to help support or protect our community. We develop automated systems to improve our ability to detect and remove abusive people and activity that may harm our community and the safety and security of our Services. If we learn of people or activity like this, we will take appropriate action by removing such people or activity or contacting law enforcement. We share information with other affiliated companies when we learn of misuse or harmful conduct by someone using our Services.*
- ***Enabling Global Access To Our Services.** To operate our global Service, we need to store and distribute content and information in data centers and systems around the world, including outside your country of residence. This infrastructure may be owned or operated by our service providers or affiliated companies.*
- ***Affiliated Companies.** We are part of the Facebook Companies. As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies as described in WhatsApp's Privacy Policy. We use the information we receive from them to help operate, provide, and improve our Services. Learn more about the Facebook Companies and their terms and polices here."*

As evident from the above, three further hyperlinks have been embedded in certain text, within the "Affiliated Companies" bullet point, as follows: "Facebook Companies", "Privacy Policy" and "here". These links operate to link the user to the following additional information:

I. The "Facebook Companies" link brings the user to an "article" on the Facebook Companies (hosted on Facebook's website). This "article" contains a number of further links to additional information, available in other linked "articles" on Facebook's website;

II. The "Privacy Policy" link brings the user back to the top of the Privacy Policy itself; and

III. The "here" link brings the user to the "article" on the Facebook Companies (hosted, as before, on Facebook's website).

c. "How We Use Information" – this links the user back to the "How We Use Information" section of the Privacy Policy. This section contains the following information:

> *"**How We Use Information***
> *We use the information we have (subject to choices you make) to operate, provide, improve, understand, customize, support, and market our Services. Here's how:*
>
> - ***Our Services.** We use the information we have to operate and provide our Services, including providing customer support, and improving, fixing, and customizing our Services. We understand how people use our Services and analyze and use the information we have to evaluate and improve our Services, research, develop, and test new services and features, and conduct troubleshooting activities. We also use your information to respond to you when you contact us.*
> - ***Safety And Security.** We verify accounts and activity, and promote safety and security on and off our Services, such as by investigating suspicious activity or violations of our Terms, and to ensure our Services are being used legally.*
> - ***Communications About Our Services And The Facebook Companies.** We use the information we have to communicate with you about our Services and features and let you know about our terms and policies and other important updates. We may provide you marketing for our Services and those of the Facebook Companies. Please see How You Exercise Your Rights for more information.*
> - ***No Third-Party Banner Ads.** We still do not allow third-party banner ads on WhatsApp. We have no intention to introduce them, but if we ever do, we will update this policy.*
> - ***Commercial Messaging.** We will allow you and third parties, like businesses, to communicate with each other using WhatsApp, such as through order, transaction, and appointment information, delivery and shipping notifications, product and service updates, and marketing. For example, you may receive flight status information for upcoming travel, a receipt for something you purchased, or a notification when a delivery will be made. Messages you may receive containing marketing could include an offer for something that might interest you. We do not want you to have a spammy experience; as with all of your messages, you can manage these communications, and we will honor the choices you make.*
> - ***Measurement, Analytics, And Other Business Services.** We help businesses who use WhatsApp measure the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services."*

As before, users are invited to receive further information by way of the links identified above. The "How You Exercise Your Rights" section may be discounted for the purpose of this assessment (given that it pertains to the exercise of the data subject rights, rather than the legal basis being relied upon for processing). The "Facebook Companies" link brings the user to the Facebook Companies "article" on Facebook's website, as before.

d. "Our Global Operations" – this links the user to the "Our Global Operations" section of the Privacy Policy. That section provides the following information:

> *"**Our Global Operations***
> *WhatsApp Ireland shares information globally, both internally within the Facebook Companies, and externally with our partners and with those you communicate around the world in accordance with this Privacy Policy. Information controlled by WhatsApp 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 Privacy Policy. These data transfers are necessary to provide the Services set forth in our Terms and globally to operate and provide our Services to you. We utilize standard contract clauses approved by the European Commission, and may rely on the European Commission's adequacy decisions about certain countries, as applicable, for data transfers from the European Economic Area to the United States and other countries.*
>
> *WhatsApp Inc. shares information globally, both internally within the Facebook Companies, and externally with businesses, service providers, and partners and with those you communicate with around the world. Your information may, for example, 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 Privacy Policy."*

As evident from the above, this section invites the user to learn more by way of three embedded hyperlinks. The only link relevant, for the purpose of the within assessment, is the link to "Terms" – this brings the user to the top of the Terms of Service. (The other links bring the user to information pertaining to standard contractual clauses and adequacy decisions located on the websites of Facebook and the European Commission).

How has the information been provided?

331. As set out above, the information, which WhatsApp asserts is provided by way of compliance with Article 13(1)(c), is provided by way of a summary in the Legal Basis Notice with links to various other documents and texts. The approach taken is somewhat disjointed in that the "summary" of the "core data uses" has been set out in very vague terms. If the user wishes to learn more, he/she must tackle the Terms of Service and also review the "Our Global Operations" section of the Privacy Policy by way of the links provided. When all of the available information has been accessed, it becomes apparent that the texts provided are variations of each other. This approach lacks clarity and concision and makes it difficult for the user to access meaningful information as to the processing operations that will be grounded on the basis of contractual necessity. By way of example, it is unclear why the "summary" of the "core data uses" could not have been prepared by reference to the contents of the "Our Services" section of the Terms of Service, with more detailed information being made available by way of a link (if a layered approach is WhatsApp's preferred approach to the delivery of the required information).

<u>Assessment of Decision-Maker</u>

332. As alluded to above, the information provided by WhatsApp, under this heading, gives rise to concern, from the perspective of the quality of information that has been provided as well as the way in which it has been provided.

Quality of information provided

333. Addressing, firstly, the quality of the information provided, it seems to me that insufficient detail has been provided in relation to the processing operations that will be grounded upon the contractual necessity basis. The language used does not enable the user to understand what way his/her personal data will be processed for each purpose. By way of example, the statement "(t)o promote safety and security" does not provide any indication as to what processing operations will be applied to the user's personal data (i.e. specifically how it will be used and in what context) to meet this objective. Further, it does not enable a sufficient understanding as to what objectives are being pursued when personal data is processed for the general purpose of "[the promotion of] safety and security". Such an approach deprives the user of meaningful information and further risks causing significant confusion as to what legal basis will be relied upon to ground a specific processing operation. Further, it is not possible to clearly identify the categories of personal data that will be processed for those processing operations that will be grounded upon contractual necessity.

The way in which information has been provided

334. Article 12(1) requires information to be 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*." The information, however, that has been provided by WhatsApp, above, has been furnished in a piecemeal fashion that requires the user to link in and out of various different sections of the Privacy Policy as well as the Terms of Service.

335. While WhatsApp suggested, in the Inquiry Submissions, that the user only needs to access the "Our Services" section of the Terms of Service (and not the entirety of the Terms of Service), the language used in the Legal Basis Notice suggests otherwise:

> *"We describe the contractual services for which this data processing is necessary in Our Services section of the Terms and in the additional informational resources accessible from our Terms."* [emphasis added]

336. Further, even if the user actively seeks out the additional information that is available by way of the various links, he/she is presented with variations of information previously furnished. By way of example, there is significant overlap between the information set out in the "How We Use Information" Section (a link to which is embedded on the "Our Legal Bases For Processing Information" sub-section of the Privacy Policy) and the contents of the "Our Services" section of the Terms of Service. Similarly, the summary of "core uses" set out in the Contractual Necessity section of the Legal Basis Notice contains a sub-set of the information provided in the "Our Services" section of the Terms of Service. The way in which the information has been spread out and included in similarly worded (linked) tranches of text means that any new elements available within a linked text could easily be overlooked by the user due to the simultaneous overlap and discrepancies between various portions of text dealing with same / similar issues in different locations. To be clear, it is not the case that the user is presented with more detailed information once he/she avails of the links provided; the information made available by way of embedded links is similar in content to the information that is available both in the primary text and other linked texts – which creates significant risk of confusion and opacity.

337. In short, the way in which the relevant information has been presented requires the user to work hard to actively engage with the original text as well as seek out the additional texts made available by way of the various links. This is unnecessary and could easily be alleviated by the adoption of a

more concise approach to the delivery of the relevant information. There does not appear to be any particular complexity to the information being delivered; the difficulties arise from the absence of a considered approach. The simple fact of the matter is that there is no single composite text or layered route available to the user such as would allow the user to quickly and easily understand the full extent of processing operations that will take place on her/her personal data on the basis of contractual necessity. Each additional layer presents the user with both similar information to that already provided as well as new elements that are not easy to detect because the language used is similar to the information that has been provided before. The user should not have to work hard to access the prescribed information; nor should he/she be left wondering if he/she has exhausted all available sources of information and nor should he/she have to try to reconcile discrepancies between the various pieces of information set out in different locations.

WhatsApp's Response to Assessment of Decision-Maker

338. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting firstly that *"(a)s people would expect, to understand the services offered under the contract users need only consult the "Our Services" section of the Terms of Service*[136]." Further, "*WhatsApp states in summary fashion for what purposes it relies on contractual necessity in [the bullet points provided] which, in themselves, serve to discharge WhatsApp's Article 13(1)(c) GDPR obligations in relation to contractual necessity*[137]."

339. WhatsApp further emphasised that:

> *"from the perspective and experience of the user, they are (1) required to agree to the Terms of Service before using the Service, which is clearly explained in the "Our Services" section of the Terms of Service; and (2) directed to the Privacy Policy and the Legal Basis Notice, which equally clearly set out the "core data uses" and other helpful information. Having been provided with this clear and comprehensive information and a link to the Terms of Service, the user is then informed that additional informational resources are available. This additional information does not undermine the information provided at (1) and (2).[138]"*

340. It further submitted that the Preliminary Draft did not take account of:

> *"the benefit to users of more generally providing a range of easily accessible tools, settings and measures to better understand the Services and how a data subject's information will be used […and …] the ease with which the user can navigate from the Privacy Policy to the linked Legal Basis Notice and to the Terms of Service (and back), and the various other links and tools available to the user at all times when using the service; nor does it take into account that these additional resources are supplemental to the information which is required to be provided under Article 13(1)(c) GDPR. These resources are not considered by WhatsApp as assisting it to discharge its Article 13(1)(c) GDPR obligations and nor should the Commission regard them as part of WhatsApp's compliance with this requirement. The information required by Article 13(1)(c) GDPR is provided in the Privacy Policy and Legal Basis Notice …"*

[136] The Preliminary Draft Submissions, paragraph 7.4
[137] The Preliminary Draft Submissions, paragraph 7.5
[138] The Preliminary Draft Submissions, paragraph 7.7

341. WhatsApp also submitted that the proposed finding "*conflicts with suggestions given by the Commission as part of its pre-GDPR engagement with WhatsApp, as evidenced in an email dated 11 April 2018, in which the Commission confirmed that the use of "technological design" and "hyperlinks to specific portions of the Terms/Privacy Policy" in the Legal Basis Notice was recommended*[139]."

342. It is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My assessment, in this regard, already takes account of the matters raised by WhatsApp in the Preliminary Draft Submissions and my concerns remain, notwithstanding WhatsApp's perspective on matters. Further, I do not agree with WhatsApp's submission concerning "*the benefit to users of more generally providing a range of easily accessible tools, settings and measures*" or "*the ease with which the user can navigate from the Privacy Policy to the linked Legal Basis Notice and to the Terms of Service (and back) …*". Such matters are only beneficial to the user if the user has been provided with the information that he/she is entitled to receive (which I do not consider to be the case here). Finally, my assessment of WhatsApp's submissions concerning its pre-GDPR engagement with the Commission's Consultation Unit has already been considered as part of my assessment of WhatsApp's Submissions of General Application, above.

Identified Legal Basis 2: Consent

What information has been provided?

343. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(a) (consent). With regard to WhatsApp's reliance on consent, the Legal Basis Notice provides that:

> *"The other legal bases we rely on in certain instances when processing your data are:*
> *…*
> *Your Consent*
> *For collecting and using information you allow us to receive through the device-based settings when you enable them (such as access to your GPS location, camera, or photos), so we can provide the features and services described when you enable the settings."*

How has the information been provided?

344. The information set out above has been provided in a clear and concise manner.

Assessment of Decision-Maker

345. While the manner in which the information has been made available to the user is clear and concise, the quality of the information provided is insufficient in that it fails to identify the processing operations that will be grounded upon the user's consent. It further fails to identify the categories of data that will be processed for the processing operations that will be grounded upon the user's consent. I note, in this regard, that the information provided specifically references the "collection" and "use" of information that the user "allows" WhatsApp to receive through the device-based settings, such as access to the user's GPS location, camera or photos.

[139] The Preliminary Draft Submissions, paragraph 7.4

346. In the "Information We Collect" section of the Privacy Policy (a link to which is embedded on the "Our Legal Bases For Processing Information" sub-section of the Privacy Policy), however, the user is informed as follows:

> - *"**Location Information.** We **collect** device location information **if you use** our location features, like when you choose to share your location with your contacts, view locations nearby or those others have shared with you, and the like, and for diagnostics and troubleshooting purposes such as if you are having trouble with our app's location features. We use various technologies to determine location, including IP, GPS, Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers."* [emphasis added]

347. While it is perfectly obvious that WhatsApp will *use* device location information if the user decides to enable his/her device-based settings so as to avail of WhatsApp's location features, it is not clear, from the above, whether WhatsApp will carry out any further processing operations and, if so, what particular processing operations, on the user's location data (as suggested by the use of the word "collect" in the text quoted above).

WhatsApp's Response to Assessment of Decision-Maker

348. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that: *"(t)he exact processing depends on the feature that is used by the user and WhatsApp provides further information in this regard, including at the time the user makes the choice. … Additionally, the categories of location data that are collected are identified in the Location Information section of the … Privacy Policy*[140]." WhatsApp further provided the consent user flows for location data, by way of an appendix to the Preliminary Draft Submissions. WhatsApp submitted, in this regard, that the user flows inform the user as to the purpose of the processing. The user flows submitted contain the following text:

User Flow 1:

> "To send a nearby place or your location, allow WhatsApp access to your location.
>
> [Options provided:] NOT NOW [or] CONTINUE"

User Flow 2:

> "Allow WhatsApp to access this device's location?
>
> [Options provided:] Deny [or] Allow

349. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of the quality of information provided. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters. I acknowledge, for example, WhatsApp's submission that the exact processing, in any case, will depend on the feature that is selected by the user. However, neither the submissions nor the sample user flows provided demonstrate that the required further information, in relation to the processing that will take place, is actually provided to the user, either at the time the user makes the choice to activate a particular feature or otherwise.

[140] The Preliminary Draft Submissions, paragraph 7.10

Identified Legal Basis 3: Legitimate Interests

What information has been provided?

350. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(f) (legitimate interests). In this regard, the Legal Basis Notice provides the following information:

> *"The other legal bases we rely on in certain instances when processing your data are:*
> *…*
> ***Our legitimate interests or the legitimate interests of a third party, where not outweighed by your interests or fundamental rights and freedoms ("legitimate interests"):***
>
> ***For people under the age of majority (under 18, in most EU countries) who have a limited ability to enter into an enforceable contract only**, we may be unable to process personal data on the grounds of contractual necessity. Nevertheless, when such a person uses our Services, it is in our legitimate interests:*
>
> - *To provide, improve, customize, and support our Services as described in Our Services;*
> - *To promote safety and security; and*
> - *To communicate with you, for example, on Service-related issues.*
>
> *The legitimate interests we rely on for this processing are:*
>
> - *To create, provide, support, and maintain innovative Services and features that enable people under the age of majority to express themselves, communicate, discover, and engage with information and businesses relevant to their interests, build community, and utilize tools and features that promote their well-being;*
> - *To secure our platform and network, verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, and keep our Services and all of the Facebook Company Products free of harmful or inappropriate content, and investigate suspicious activity or violations of our terms or policies and to protect the safety of people under the age of majority, including to prevent exploitation or other harms to which such individuals may be particularly vulnerable.*
>
> ***For all people, including those under the age of majority:***
>
> - ***For providing measurement, analytics, and other business services where we are processing data as a controller.** The legitimate interests we rely on for this processing are:*
>   - *To provide accurate and reliable reporting to businesses and other partners, to ensure accurate pricing and statistics on performance, and to demonstrate the value our partners realise using our Services; and*
>   - *In the interests of businesses and other partners to help them understand their customers and improve their businesses, validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services.*
>
> - ***For providing marketing communications to you.** The legitimate interests we rely on for this processing are:*
>   - *To promote Facebook Company Products and issue direct marketing.*

- ***To share information with others including law enforcement and to respond to legal requests.*** *See our Privacy Policy under Law and Protection for more information. The legitimate interests we rely on for this processing are:*
    - *To prevent and address fraud, unauthorised use of the Facebook Company Products, violations of our terms and policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), our users or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm.*

- ***To share information with the Facebook Companies to promote safety and security.*** *See our Privacy Policy under "How We Work with Other Facebook Companies" for more information. The legitimate interests we rely on for this processing are:*
    - *To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products."*

351. The text contains a number of embedded links which, when selected, bring the user to the following text/information:

    a. The "Our Services" section of the Terms of Service (which has further links to the "Facebook Companies" and the "Privacy Policy");

    b. An "article", hosted on Facebook's website, entitled "Facebook Company Products" (containing further links to other relevant/related "articles", on Facebook's website);

    c. The "Law And Protection" section of the Privacy Policy;

    d. The "How We Work With Other Facebook Companies" section of the Privacy Policy, with a further link to a Frequently Asked Question ("**FAQ**") on this topic ("the **Facebook FAQ**[141]");

    e. An "article", hosted on Facebook's website, entitled "Facebook Companies" (containing further links to other relevant/related "articles", on Facebook's website).

How has the information been provided?

352. The information has been provided largely by way of the relevant section of the Legal Basis Notice with links to a number of other documents and texts. As before, the approach taken is somewhat disjointed (albeit to a lesser degree than the contractual necessity section). As before, it is unclear why the summary of core data uses referenced under the section that addresses those users under the age of majority could not have been prepared by reference to the contents of the "Our Services" section of the Terms of Service, with more detailed information being made available by way of a link (if a layered approach is WhatsApp's preferred approach to the delivery of the required information).

Assessment of Decision-Maker

353. As before, the information provided under this heading gives risk to concern, from the perspective of the quality of information that has been provided as well as the way in which it has been provided.

Quality of information provided

[141] Available at https://faq.whatsapp.com/general/26000112/?eea=1 (the "**Facebook FAQ**")

354. It seems to me that insufficient detail has been provided in relation to the processing operations that will be grounded upon the legitimate interests basis. Further, it is not possible to identify what categories of personal data will be processed for those processing operations that will be grounded upon this legal basis.

The way in which information has been provided

355. The information has been furnished in a piecemeal fashion that requires the user to link in and out of various different sections of the Privacy Policy as well as the Terms of Service and a comprehensive FAQ entitled "How we work with the Facebook Companies"[142] (available by way of a link from the linked "How We Work With Other Facebook Companies" section of the Privacy Policy). As before, this results in a situation whereby, even if the user actively seeks out the additional information that is available by way of the various links, he/she is presented with variations of information previously furnished. The way in which the information has been spread out and included in similarly worded tranches of text means that any new elements available within a linked text could easily be overlooked by the user due to the simultaneous overlap and discrepancies between various portions of text dealing with the same / similar issues in different locations. This is unnecessary and could easily be alleviated by adopting a concise approach to the delivery of the relevant information.

356. As before, there is no single composite text or layered route available to the user such as would allow the user to quickly and easily understand the full extent of processing operations that will be conducted on her/her personal data in reliance on the legitimate interests legal basis. Each additional layer presents the user with similar information to that already provided as well as new elements that are not easy to detect. The user should not have to work hard to access the prescribed information; nor should he/she be left wondering if they have exhausted all available sources of information and nor should he/she have to try to reconcile discrepancies between the various pieces of information given in different locations.

357. I also note, in this regard, that the Terms of Service appears to contradict the information set out in the Legal Basis Notice, in relation to reliance on the legitimate interests basis for processing the personal data of users who have not attained the age of majority. The Legal Basis Notices states, in this regard, that the legitimate interests basis will ground processing operations in cases where the user concerned has a limited ability to enter into an enforceable contract. The Terms of Service, however, provides, in the "About Our Services" section, that:

> *"Age. If you live in a country in the European Region, you must be at least 16 years old to use our Services or such greater age required in your country to register for or use our Services. … . In addition to being of the minimum required age to use our Services under applicable law, if you are not old enough to have authority to agree to our Terms in your country,* ***your parent or guardian must agree to our Terms on your behalf****." [emphasis added]*

358. Thus, while the information provided suggests that inability to enter into a contract might mean that WhatsApp will not be able to rely on the contract legal basis for any consequent processing of personal data, the Terms of Service clearly require a contract to be entered into, if necessary, by a parent or guardian acting on behalf of the user concerned. This appears to be somewhat of a contradiction in terms.

[142] Available at https://faq.whatsapp.com/general/26000112/?eea=1 (the "**Facebook FAQ**")

359. Further, the bullet point summary of processing operations set out under this legitimate interests heading includes three of the four operations listed under the contractual necessity heading. If it is the case that the legitimate interests basis will form the basis for processing in the case of those under the age of majority, it is unclear why reference to "the transmission, storage and processing of data outside of the EEA" has been omitted from this summary list.

360. I further note that a number of the objectives set out in the general body of the legitimate interests section have already been included in the contractual necessity section. Similarly, by incorporating a link to the "Law And Protection" section, this indicates that the legitimate interests basis will form the basis for any processing set out in this text, including for the purpose of "[responding] pursuant to applicable law or regulations, to legal process, or to government requests". The same issue arises in relation to the incorporation of a link to the "How We Work With Other Facebook Companies" section of the Privacy Policy. I note, in this regard, that such processing has also been included under the contractual necessity heading. This state of affairs leaves the user unable to identify which legal basis is being relied upon when processing his/her personal data for any required processing activities.

WhatsApp's Response to Assessment of Decision-Maker

361. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that the provision of additional information through links "*does not undermine the information made available in the Legal Basis Notice but rather helps the user better understand the Service and how a data subject's information will be used. A reduction of information or removing convenient hyperlinks to relevant information would have the effect of reducing overall user understanding and control of the Service, to the detriment of users*[143]".

362. In relation to my observation that "*a number of the objectives set out in the general body of the legitimate interests section have already been included in the contractual necessity section … This state of affairs leaves the user unable to identify which legal basis is being relied upon …*", WhatsApp's position is that it "*has designed the Legal Basis Notice in this manner, as depending on the circumstances, more than one legal basis for processing may be applicable to processing pursuing the same objective. … WhatsApp is being transparent about the fact that it relies on different legal bases in different circumstances, and does not consider this should be a point of criticism*[144]."

363. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp under this heading. I have already set out, above, the reasons why I consider the information provided to be insufficient, in terms of quality and manner of delivery. That assessment already takes account of the matters raised by WhatsApp in the Preliminary Draft Submissions and my concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters. I remain particularly concerned about the position whereby the data subject is unable to identify, from the information provided, which legal basis is being relied upon to support what particular processing operation.

[143] The Preliminary Draft Submissions, paragraph 7.14
[144] The Preliminary Draft Submissions, paragraph 7.16

Identified Legal Basis 4: Compliance with a Legal Obligation

What information has been provided?

364. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(c) (compliance with a legal obligation). In this regard, the Legal Basis Notice provides the following information under this heading:

> *"The other legal bases we rely on in certain instances when processing your data are:*
> *…*
> *For processing data when the law requires it, including, for example, if there is a valid legal request for certain data. See our Privacy Policy under Law and Protection for more information."*

365. The "Law And Protection" section of the Privacy Policy further provides as follows:

> *"**Law And Protection***
> *We collect, use, preserve, and share your information if we have a good-faith belief that it is reasonably necessary to: (a) respond pursuant to applicable law or regulations, to legal process, or to government requests; (b) enforce our Terms and any other applicable terms and policies, including for investigations of potential violations; (c) detect, investigate, prevent, and address fraud and other illegal activity, security, or technical issues; or (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook Companies, or others, including to prevent death or imminent bodily harm."*

How has the information been provided?

366. The information has been provided by way of a short statement in the body of the Legal Basis Notice with a link to a short text in the "Law And Protection" section of the Privacy Policy, as referred to above.

Assessment of Decision-Maker

Quality of information provided

367. I note that the "Law And Protection" section has already been incorporated, by way of a link, into the legitimate interests section. In these circumstances, its incorporation into the "legal obligations" section is a source of potential confusion for the user. I further note that, while the "Law And Protection" section identifies some processing operations ("collect", "preserve" and "share"), it is not clear what processing operations might be covered by the umbrella term "use". Further, and while I acknowledge that the processing that might be necessitated in the circumstances covered by this heading is largely dependent on the occurrence of certain events, the user should be provided with some indication as to what categories of personal data might be processed under this heading.

368. I note, in this regard, that there is information available elsewhere on the WhatsApp website that might assist the user to understand how and why his/her personal data might be processed under this heading. There are links within the Privacy Policy (embedded in text such as "end-to-end encrypted") that links the user to WhatsApp's "End-to-end encryption" FAQ[145]. There are a series of

[145] Available at https://faq.whatsapp.com/en/general/28030015

further links within that document, including one that links to an "Information for Law Enforcement Authorities" FAQ[146]. While I note that this document does not appear to be directed to EEA users (given that it only references WhatsApp, Inc., rather than WhatsApp), it provides useful information about the circumstances in which WhatsApp might have to share information with law enforcement authorities. Given the requirement for the data controller to provide "meaningful" information to the data subject, I recommend that consideration is given to a more direct incorporation of this document (with appropriate references to WhatsApp) or, at the very least, the incorporation of similar information, into the Privacy Policy (insofar as the information proffered in that document might be applicable).

369. I am further of the view that, where WhatsApp intends to ground a processing operation on this legal basis, it should also identify the "European Union law or Member State law" giving rise to the obligation for WhatsApp to process data.

The way in which information has been provided

370. The requirements of Article 12(1) are clear in that any prescribed information must be provided in a *"concise, transparent, intelligible and easily accessible form, using clear and plain language …"*. The information that has been provided by WhatsApp, however, is somewhat opaque and does not enable the user to understand the circumstances in which his/her personal data will be processed under this heading.

WhatsApp's Response to Assessment of Decision-Maker

371. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that *"(t)he reality is that the processing described in the "Law and Protection" section may be based on legal obligation or legitimate interest depending on the circumstances at hand*[147]*"*.

372. Further, *"(i)n light of the sensitive and often complex processing that occurs for law enforcement purposes, the description of the processing (considered together, i.e. "collect, use, preserve and share") in combination with the rest of the section gives users a clear picture of the ways in which their data may be "used". While "use" is a broad term, when read together with the rest of the section, WhatsApp considers it is sufficiently clear*[148]*."*

373. Again, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters.

374. While my view, as set out in paragraph 369 above, that information should be provided in relation to any underlying legal obligation set out in EU or Member State law, was not included in the Preliminary Draft, in the context of my assessment of Article 13(1)(c) concerning WhatsApp's reliance on the legal obligation legal basis, it was however included in the context of my assessment of the information

[146] Available at https://faq.whatsapp.com/en/general/26000050
[147] The Preliminary Draft Submissions, paragraph 7.17
[148] The Preliminary Draft Submissions, paragraph 7.18

provided under the heading "Identified Legal Basis 6: Tasks carried out in the public interest". Given that Article 6(3) is the origin for this requirement, in both cases, I am appraised of WhatsApp's position on the issue by virtue of the submissions that it furnished in response to my assessment of "Identified Legal Basis 6: Tasks carried out in the public interest". In the circumstances, my response to those submissions, as set out in paragraphs 394 – 398, below, applies equally here.

375. WhatsApp, by way of its Article 65 Submissions, expressed the view that my conclusion, as regards the requirement for a data controller to identify the European Union law or Member State law giving rise to the relevant obligation is "flawed in substance" on the basis, *inter alia*, that[149]:

    a. "The legislature specifically prescribed that such information be provided in Article 13(1)(d) GDPR, and the fact that it did not choose to do the same with respect to Article 13(1)(c) is significant."

    b. "There are also straightforward reasons to justify drawing a distinction between these provisions. For example, it is feasible for controllers when preparing a privacy policy to identify the legitimate interests they are pursuing to process data under Article 6(1)(f) GDPR, in a way which would not be the case if controllers were required to exhaustively identify in their privacy policy all legal obligations that may justify them processing data pursuant to Articles 6(1)(c) and/or 6(1)(e) GDPR. This is because a controller decides (and so can readily identify) the legitimate interests it wishes to rely on pursuant to Article 6(1)(f) GDPR; however a controller does not decide which legal obligations it is subject to and which may be relevant to Articles 6(1)(c) and/or 6(1)(e) GDPR given this is the responsibility of law makers, both at EU level and national level."

    c. "The Commission's approach would be infeasible for controllers. For example, in Ireland, various regulatory bodies have a wide range of powers to request information from entities such as [WhatsApp], and these powers change at the discretion of the Irish legislature. On top of this, a multitude of regulatory bodies from across other EU Member States also have a wide range of powers to request information – again at the discretion of their legislatures – which they might consider would also apply to entities such as [WhatsApp]. It is not feasible as a matter of practice for a controller to identify all such laws in existence when preparing a privacy policy. Indeed it may be the case that the controller only becomes aware of a particular legal obligation at the time when such powers are exercised, once it is put on notice and after it has had the opportunity to consider their applicability on the facts of a specific request. The approach prescribed by the Commission therefore risks imposing obligations on controllers which would be impossible to comply with."

    d. A similar issue arises with respect to Irish criminal laws, where laws which may give rise to a requirement to produce information to law enforcement are spread across numerous pieces of primary and secondary legislation. As one illustration of this, the Law Reform Commission reported that as of 2015, more than 300 separate legislative provisions … provide for powers to issue search warrants. It simply cannot have been the legislative intention to exhaustively list all such legal obligations that a controller is subject to in order to comply with its obligations under Article 13(1)(c) GDPR."

[149] The Article 65 Submissions, paragraphs 53.1 to 53.7

e. Even if controllers were able to identify all such relevant legal obligations in advance, the long list of names of statutory provisions that would then need to be provided to data subjects would serve only to overwhelm them with detailed – and, for most practical purposes, useless – information." WhatsApp has further submitted, in this regard, that, in the event that I consider "such information regarding laws" to be required by Article 13(1)(c), I should conclude that it would be "more beneficial for data subjects if controllers were to, at most, describe the *categories* or *types* of laws engaged, and explain how these categories or types of laws could result in the processing of their data". WhatsApp considers that this is the "only way in which such information could feasibly be provided by controllers and be meaningful for a data subject."

376. I note that I have already addressed the matters covered by the submissions summarised at paragraph 375(a), above, as part of the same assessment carried out for the purpose of the information required to be provided where a data controller intends to process personal data on the basis of Article 6(1)(e) (tasks carried out in the public interest). I remain of the views set out in paragraphs 394 to 398, below.

377. As regards the submissions set out at paragraph 375(b), above, I disagree that the fact that a controller does not decide which legal obligations it is subject to is a relevant consideration. If a data controller processes personal data in pursuit of compliance with a legal obligation, then the controller is in a position to "readily identify" and inform the data subjects concerned about the processing and the reason for the processing. To be clear, it is not the case, as appears to be suggested by WhatsApp's submissions, that a data controller is required to "*exhaustively identify … all legal obligations that **may** justify them processing data pursuant to Articles 6(1)(c) and/or 6(1)(e) GDPR*" [emphasis added]. A controller either processes personal data pursuant to a requirement set out in EU or Member State law or it does not; if it does, then all that is required is for the controller to inform the data subjects concerned about that processing along with the underlying legal requirement.

378. I further do not agree that such a requirement would be "infeasible" for controllers, as suggested. If it is the case that a controller becomes subject to a new legal requirement to process personal data, then all that is required is for the data controller to update its privacy policy to reflect that. It is important to remember, in this regard, that the transparency obligation is an ongoing one and not one which can be complied with on a once-off basis. As with all of the obligations that are imposed on data controllers, the GDPR requires controllers to continually monitor and review their practices to ensure ongoing compliance with the obligations arising. This is particularly the case for the transparency obligation, which is not only one of the core data subject rights but also one of the fair processing principles enshrined in Article 5 of the GDPR. While I note WhatsApp's reference to a 2015 report from the Law Reform Commission, identifying more than 300 separate legislative provisions providing for powers to issue search warrants, it is unlikely to be the case that WhatsApp is subject to a requirement to process personal data pursuant to each one of those provisions.

379. As regards the suggestion that a requirement to provide information as to the underlying legal obligation would result in the data subject being overwhelmed with "details – and, for most practical purposes, useless – information", I firstly disagree that such information is appropriately classified as "useless". The information enables the data subject to understand why his/her personal data is being processed, thereby enabling him/her to (i) hold the relevant controller accountable and (ii) exercise

his/her data subject rights, if he/she wishes to do so. I secondly disagree that a requirement to provide such information will result in the data subject being overwhelmed with "details". As noted above, all a controller is required to do is identify any legislative provisions pursuant to which it (actually, rather than potentially) processes personal data. Once this information is provided in a clear and concise manner (as required by Article 12), it is difficult to see how this would operate to overwhelm a data subject. Accordingly, I do not agree that it would be necessary or appropriate for me to conclude that it would be more beneficial for data subjects if controllers were to "at most, describe the *categories* or *types* of law engaged, and explain how these categories or types of laws could result in the processing of their data", as suggested by WhatsApp.

Identified Legal Basis 5: The vital interests of the data subject or those of another person

What information has been provided?

380. In this section, I examine whether there has been compliance with Article 13(1)(c) insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(d) (vital interests of the data subject or another person). In this regard, the Legal Basis Notice provides the following information under this heading:

> *"The other legal bases we rely on in certain instances when processing your data are:*
> *…*
> *The vital interests we rely on for this processing include protection of your life or physical integrity or that of others, and we rely on it to combat harmful conduct and promote safety and security, for example, when we are investigating reports of harmful conduct or when someone needs help."*

How has the information been provided?

381. The information has been provided by way of the above statement.

Assessment of Decision-Maker

382. I note that the text quoted above suggests that the vital interests basis will be used to ground processing in the context of combatting "harmful conduct" and to "promote safety and security, for example, when we are investigating reports of harmful conduct". Given that these objectives have already been referenced in the contractual necessity and legitimate interests sections, the expected processing operation(s) should be set out with greater granularity so that the user can identify which 'safety and security' objectives will be grounded on vital interests, as distinct from other similar objectives for which another legal basis is relied on. Further, the user should be provided with some indication of what categories of his/her personal data might need to be processed under this heading. Again, I appreciate that the processing that might be necessitated under this heading is entirely dependent on the occurrence of particular events however WhatsApp should be able to, at the very least, provide the user with some examples of the type of data that has been processed by reference to the vital interests legal basis in the past.

WhatsApp's Response to Assessment of Decision-Maker

383. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that it does not consider that:

"more granularity is required to comply with Article 13(1)(c) GDPR in this regard. In particular, WhatsApp is of the view that the user is already provided with adequate information so that the user can identify which "safety and security" objectives will be grounded on vital interests … as it is evident that this will be engaged in circumstances where a life or physical integrity is at risk." Nonetheless, WhatsApp intends to provide the user with some examples of the type of data that has been processed by reference to past processing, as suggested by the Commission.[150]"

384. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of the quality of the information that has been provided. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters however I acknowledge that WhatsApp intends to provide the user with examples, as suggested.

Identified Legal Basis 6: Tasks carried out in the public interest

What information has been provided?

385. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(e) (tasks carried out in the public interest). In this regard, the Legal Basis Notice provides the following information under this heading:

> *"The other legal bases we rely on in certain instances when processing your data are:*
> *…*
> *For undertaking research and to promote safety and security, as described in more detail in our Privacy Policy under How We Use Information, where this is necessary in the public interest as laid down by European Union law or Member State law to which we are subject."*

How has the information been provided?

386. The information has been provided by way of the statement set out above with a link that, when selected, brings the user back to the "How We Use Information" section of the Privacy Policy. While that section contains two further embedded links, the one relevant to this assessment brings the user to an "article" hosted on the Facebook website entitled "the Facebook Companies" (which contains further links to further relevant information).

Assessment of Decision-Maker

Quality of information provided

387. I am unable to identify at any level, based on the information that has been provided in relation to this legal basis, what sort of processing operation will be grounded on this legal basis and what categories of personal data will be processed under this heading. Where WhatsApp intends to ground a processing operation on this legal basis, it should also identify the "European Union law or Member State law" giving rise to the obligation for WhatsApp to process data.

388. I further note that "the promotion of safety and security" has been included under the contractual necessity heading, the legitimate interests heading and the vital interests heading. If this is not an

[150] The Preliminary Draft Submissions, paragraph 7.21

error, WhatsApp must identify, with sufficient granularity, the relevant processing operation(s) that will be carried out, under each heading, for the purpose of the promotion of safety and security.

The way in which information has been provided

389. Further, it is unfortunate that the way in which the information has been provided is somewhat circular in that:

    a. The user is linked to the Legal Basis Notice by the "Our Legal Basis For Processing Information" section of the Privacy Policy. The top of that section includes a link back to the "How We Use Information" section of the Privacy Policy.

    b. Thus, the inclusion of a link back to the "How We Use Information" section of the Privacy Policy does not provide the user with any new or more detailed information but merely brings the user in a circle back to the original starting point.

390. WhatsApp is perfectly entitled to incorporate layering into its approach to the delivery of information. In order for this to be effective, however, it must be done in a considered way such that the information being provided, across the various layers, still meets the requirements of Article 12(1) for information to be provided in a "*concise, transparent, intelligible and easily accessible form*". Bringing the user on a pointless circuitous route, as detailed above, does not achieve this.

WhatsApp's Response to Assessment of Decision-Maker

391. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting firstly that:

> *"WhatsApp does not consider a requirement can be construed under Article 13(1)(c) GDPR to exhaustively list in a privacy policy-type document all the EU or Member State laws potentially engaged when a controller might rely on Article 6(1)(e) as a legal basis to process personal data. We would question whether it is even possible to identify in advance every such applicable law. Additionally, if this were the case, when new laws are enacted at EU or Member State level that might impose a duty on WhatsApp to carry out tasks in the public interest, WhatsApp would have to update its Privacy Policy each time. This would be impractical to implement, particularly where an applicable situation develops at pace (which could very well be the case in circumstances of public interest). This would be confusing for users, would be likely to create information fatigue, and would not be proportionate to WhatsApp's obligations under the GDPR[151]."*

392. It further submitted that *"… for the same reasons, WhatsApp does not consider there can be a requirement to specify with granularity the processing operations that will take place under "the promotion of safety and security" heading*[152]*."*

393. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the

[151] The Preliminary Draft Submissions, paragraph 7.22
[152] The Preliminary Draft Submissions, paragraph 7.24

manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters.

394. In relation to WhatsApp's submission that Article 13(1)(c) does not require the identification of the underlying EU or Member State law, I note that it is firstly clear, from Article 6(3) (and Recital 45), that, in order for a controller to be able to process personal data in reliance upon Article 6(1)(e), the basis for the processing must be laid down by EU or Member State law. The existence of such legal underpinning is therefore a component part of reliance upon Article 6(1)(e).

395. Article 13(1)(c) requires the provision of information concerning the "legal basis for the processing". It is clear, from Article 6(3), that the underlying EU or Member State law forms the basis of processing carried out in reliance on Article 6(1)(e). That being the case, my view is that, where a controller intends to process personal data in reliance on Article 6(1)(e), Article 13(1)(c) requires the controller to inform the data subject not only of its intended reliance on Article 6(1)(e), but also of the EU or Member State law that forms the underlying basis for the processing concerned.

396. I note that such an approach is consistent with the purpose of the transparency obligation, as considered as part of the assessment that led to the formulation of the Proposed Approach, above. I note, in particular, the role of transparency in helping the data subject to hold the data controller accountable.

397. I further note that Article 13 already indicates that this is the correct approach, by reference to the requirement, set out in Article 13(1)(d), for the controller to identify the legitimate interests being pursued in a case where the processing is grounded upon Article 6(1)(f). The existence of a legitimate interest plays a similar role, in the context of Article 6(1)(f), as that played by the underlying EU or Member State law, in the context of Article 6(1)(e). That being the case, it would not make sense for Article 13 to require the identification of the legitimate interest being pursued, in the case of processing grounded upon Article 6(1)(f), but not the underlying EU or Member State law that forms the basis for processing grounded upon Article 6(1)(e).

398. Finally, and insofar as it might be suggested that the above approach is inconsistent with the principle of *expressio unius est exclusio alterius* (on the basis that the express inclusion of the requirement to provide information about the legitimate interest being pursued suggests that the legislator did not intend for Article 13 to contain a similar requirement as regards the provision of information concerning any underlying legal requirement enshrined in EU or Member State law), I note that it is not possible to rely on Article 6(1)(c) or (e) in the abstract; both are subject to compliance with the provisions of Article 6(3). This is not the case with Article 6(1)(f), which is self-contained and not subject to any additional and specific conditionality within Article 6 itself. This means that, in the context of Article 13, it was not necessary for the legislator to specifically require the provision of information as to the underlying EU or Member State law where the applicable legal basis is Article 6(1)(c) or 6(1)(e); this requirement has already been incorporated into these provisions by Article 6(3). The absence of such a corresponding provision in the context of Article 6(1)(f) meant that it was necessary for the legislator to specifically incorporate a requirement for information to be provided about the underlying legitimate interest where, pursuant to Article 13(1)(c), the data controller has confirmed its intention to rely on Article 6(1)(f) to ground its processing.

Finding: Article 13(1)(c) – The purposes of the processing for which the personal data are intended as well as the legal basis for the processing

399. **For the reasons set out in the assessment sections above, I find that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c) and Article 12(1).**

Article 13(1)(d) – where applicable, the Legitimate Interests being pursued

Required Information and WhatsApp's Response to Investigator's Questions

400. Article 13(1)(d) requires a data controller, "*where the processing is based on [the legitimate interests ground]" to provide information to the data subject in relation to "the legitimate interests being pursued by the controller or by a third party*".

401. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

> *"[WhatsApp] identifies legitimate interests pursued in the 'How We Process Your Information' notice."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

402. The Investigator set out her views in relation to the extent to which WhatsApp complies with its obligation under this heading by reference to **Proposed Findings 8 and 9**.

403. By reference to **Proposed Finding 8**, the Investigator considered the information that had been provided under this heading, where that information was "addressed specifically to a child". The Investigator expressed the view, in this regard, that the language used "in relation to the legitimate interests pursued when processing the personal data of people under the age of majority is unchanged from the vocabulary, tone and style of the information utilised throughout the "How We Process Your Information" Notice." Accordingly, the Investigator proposed a finding that the language of the information provided under Article 13(1)(d) was "not in line with the requirements of clarity for people under the age of majority, in contravention of Article 12(1) of the GDPR".

404. WhatsApp disagreed with the Investigator's views. It submitted[153] that:

> *"… the Draft Report refers to "children" throughout but does not acknowledge that the WhatsApp Terms of Service require users in the European Region to be at least 16 years old to use the service. This is an important consideration as what information can be understood by a 16 year old is likely very different from that which can be understood by a 13 year old, and the [Investigator] appears to have taken no account of this."*

405. The Investigator countered that "in the absence of such a distinction in the GDPR or in the Transparency Guidelines, the guidelines regarding communication with a child remain applicable in respect of communications addressed specifically to persons aged 16 or 17 years old." She confirmed her view, by way of Conclusion 8, that "the language of the information provided under Article

[153] The Inquiry Submissions, paragraph 10.2

13(1)(d) of the GDPR is not in line with the requirements of clarity for people under the age of majority, in contravention of Article 12(1) of the GDPR."

406. By reference to **Proposed Finding 9**, the Investigator expressed the view that the Article 13(1)(d) requirement to identify the legitimate interests being pursued was:

> *"a cumulative requirement, which results in Articles 13(1)(c) and 13(1)(d) operating together to place upon the data controller a requirement to set out the purposes of the processing in relation to the legitimate interests legal basis, along with the legitimate interests being pursued in carrying out the processing operations."*

407. The Investigator formed the view that the Legal Basis Notice "[conflated] the purposes of the processing of personal data with the legitimate interests relied upon to process personal data, without setting out any specific information in relation to the processing operation(s) or set of operations involved."

408. Accordingly, the Investigator proposed a finding that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

409. WhatsApp disagreed with the Investigator's views. It submitted[154] that:

> *"In assessing the adequacy of the information provided, the Draft Report also fails to take into account that the description of the purpose of the processing will often, in and of itself, necessarily identify the nature of the legitimate interest in issue. The proposed finding is also based on a mischaracterisation of the obligation on a controller under Article 13(1)(c) – i.e. there is no need to specify "processing operations" … ."*

410. The Investigator was unconvinced by WhatsApp's submissions and confirmed her view, by way of Conclusion 9, that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

Assessment of Decision-Maker: What information has been provided?

411. The information provided has been detailed above (in the "legitimate interests" section of the Article 13(1)(c) assessment) and can be found in the Legal Basis Notice.

Assessment of Decision-Maker: How has the information been provided?

412. The information has been provided by way of a series of bullet points, under identified objectives (that need to be detailed with greater specificity, as discussed under the Article 13(1)(c) assessment, above). In this way, the user can clearly identify which legitimate interests are being pursued under each identified objective. The information itself has been provided in a meaningful manner, such that the user is enabled to understand the legitimate interests being pursued. While I note that the Investigator expressed concern about the lack of clarity concerning whether the legitimate interests being pursued were those of WhatsApp or a third party, I do not share those concerns in circumstances where the information provided includes indications as to the "owner" of the legitimate interests such as:

[154] The Inquiry Submissions, paragraph 11.1

- "... it is in **our** legitimate interests [to ...]" [emphasis added];
- "In the interests of **business and other partners** ..." [emphasis added]; and
- The inclusion of express reference to the "Facebook Companies" where the interests being pursued include those of the Facebook Companies.

Finding: Article 13(1)(d) – where applicable, the Legitimate Interests being pursued

413. I expressed the view, in the Composite Draft, that WhatsApp had comprehensively addressed its obligations under Article 13(1)(d), insofar as it was my expressed position that the information provided is clear and transparent and provides the data subject with a meaningful overview of the legitimate interests being relied upon when processing personal data under this heading. Accordingly, the Composite Draft proposed a finding that WhatsApp had complied, in full, with the requirements of Article 13(1)(d).

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

414. The German (Federal), Polish and Italian SAs each raised an objection to the above described finding which was proposed in the Composite Draft under this particular heading. The objections collectively identified various concerns as to the sufficiency of the information that has been provided by WhatsApp for the purpose of Article 13(1)(d).

415. 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 mechanism. Having considered the merits of the objections, the Board determined[155] as follows:

> *50. "The EDPB recalls that where legitimate interest (Article 6(1)(f) GDPR) is the legal basis for the processing, information about the legitimate interests pursued by the data controller or a third party has to be provided to the data subject under Article 13(1)(d) GDPR.*
>
> *51. As recalled in the Transparency Guidelines, the concept of transparency under the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles [156]. The Transparency Guidelines go on to explain that the practical (information) requirements are outlined in Articles 12 - 14 GDPR and remark that the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects [157].*
>
> *52. With regard to Article 13(1)(d) GDPR the Transparency Guidelines state that the **specific interest** [158] in question must be identified for the benefit of the data subject.*
>
> *53. In this light, the EDPB recalls the wording of Article 13(1)(d) GDPR, which reads that information shall be provided to the data subject "where the processing is based on point*

[155] The Article 65 Decision, paragraphs 42 to 66 (inclusive)
[156] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4 (page 5). This passage was also recalled by the Draft Decision in paragraph 291.
[157] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4 (page 5).
[158] Footnote from the Article 65 Decision: Transparency Guidelines, annex, page 36.

(f) of Article 6(1) GDPR" - about "the legitimate interests pursued by the controller or by a third party".

54. The EDPB notes that the nature of Article 13(1)(d) GDPR (like Article 13(1)(c) GDPR) expressis verbis relates to the specific processing [159]. In this context the EDPB also recalls the broad wording with which Recital 39 GDPR describes transparency obligations.

55. Furthermore, the EDPB considers that the purpose of these duties of the controller is to ***enable data subjects to exercise their rights under the GDPR*** *[160], such as the right to object pursuant to Article 21 GDPR, which requires the data subject to state the grounds for the objection relating to his or her particular situation. This is elaborated on in the Draft Decision by the IE SA with regard to the requirements of Article 13(1)(c) GDPR. There the IE SA correctly identifies that:*

> *"(a) a data controller will usually collect different categories of personal data from an individual data subject at different times, in different ways and for different purposes [...];*
>
> *(b) a data controller will always need to carry out more than one processing operation in order to achieve the stated purpose of a processing operation; and*
>
> *(c) a data controller might collect a particular category of data for a number of different purposes, each supported by a different legal basis" [161].*

56. The EDPB is of the view, as outlined in the draft decision, [162] that providing full information on each and every processing operation respectively is the only approach that will ensure that the data subjects can:

> *(a) exercise choice as to whether or not they might wish to exercise any of their data subject rights and, if so, which one(s);*
>
> *(b) assess whether or not they satisfy any conditionality associated with the entitlement to exercise a particular right;*
>
> *(c) assess whether or not they are entitled to have a particular right enforced by the data controller concerned; and*
>
> *(d) assess whether or not they have a ground of complaint such as to be able to meaningfully assess whether or not they wish to exercise their right to lodge a complaint with a supervisory authority.*

57. However, the EDPB notes that these same arguments also are to be considered when assessing the information under Article 13(1)(d) GDPR. With regard to the information provided under Article 13(1)(d) GDPR the EDPB therefore agrees with the objections insofar as in order for the data subject to properly exercise their rights under the GDPR, specific information about what legitimate interests relate to each processing operation, and about which entity pursues each legitimate interest, is necessary [163]. Without this information, the data subject is not properly enabled to exercise his or her rights under the GDPR.

---

[159] Footnote from the Article 65 Decision: See also Recitals 60 and 61 GDPR.
[160] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4 (page 5).
[161] Footnote from the Article 65 Decision: Draft Decision, paragraph 299.
[162] Footnote from the Article 65 Decision: Draft Decision, paragraph 300 (see also 299 f.).
[163] Footnote from the Article 65 Decision: Draft Decision, paragraph 392-393.

58. The provided information therefore has to meet these requirements in order to be compliant with Article 13(1)(d) GDPR.

59. The EDPB notes that overall the Legal Basis Notice consists of a list of several objectives under which WhatsApp IE has provided several legitimate interests, usually in the manner of bullet points, as was identified by the IE SA. The EDPB considers that in the Legal Basis Notice WhatsApp IE has not specified the provided information with regard to the corresponding processing operation such as information about what categories of personal data are being processed for which processing pursued under basis of each legitimate interest respectively. The Legal Basis Notice does not contain such specific information in relation to the processing operation(s) or set of operations involved [164].

60. This is in line with the arguments brought forward by the CSAs' relevant objections, and the EDPB notes that this described lack of information negatively impacts data subjects' ability to exercise their rights under the GDPR, such as the Right to Object under Article 21 GDPR [165].

61. Furthermore, the EDPB notes that several passages from the Legal Basis Notice, including those with regard to persons under the age of majority, among which the examples being brought forward in the objection of the DE SA (like "For providing measurement, analytics, and other business services") do not meet the necessary threshold of clarity and intelligibility that is required by Article 13(1)(d) GDPR in this case [166].

62. The EDPB notes the similarities between the examples of non-transparent ("poor practice") information put forward in the Transparency Guidelines [167] and the Legal Basis notice of WhatsApp IE, which includes for example: "For providing measurement, analytics, and other business services where we are processing data as a controller [...]" [168]; "The legitimate interests we rely on for this processing are: [...] In the interests of businesses and other partners to help them understand their customers and improve their businesses, validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services" [169].

63. Under these circumstances the data subjects are not in a position to exercise their data subject rights, since it is unclear what is meant by "other business services", as WhatsApp IE does not disclose this information or provide a relation to the specific legitimate interest. The EDPB also notes that it is unclear which businesses or partners WhatsApp IE refers to.

64. The EDPB also takes note of the fact that descriptions of the legitimate interest as the basis of a processing like "[t]o create, provide, support, and maintain innovative Services and features [...]" [170] do not meet the required threshold of clarity required by Article 13(1)(d) GDPR, as they do not inform the data subjects about what data is used for what

[164] Footnote from the Article 65 Decision: This was also initially found by the IE SA at the investigation stage. Draft Decision, paragraph 393.
[165] Footnote from the Article 65 Decision: This also corresponds to the findings with regard to the infringement of Article 13(1)(c) GDPR as elaborated in the Draft Decision.
[166] Footnote from the Article 65 Decision: Draft Decision, paragraph 341.
[167] Footnote from the Article 65 Decision: Transparency Guidelines, p. 9. Examples of "poor practice" mentioned by the Guidelines are: "*We may use your personal data to develop new services*" (as it is unclear what the "services" are or how the data will help develop them); "*We may use your personal data for research purposes* (as it is unclear what kind of "research" this refers to); and "We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails)".
[168] Footnote from the Article 65 Decision: Draft Decision, paragraph 341.
[169] Footnote from the Article 65 Decision: Draft Decision, paragraph 341.
[170] Footnote from the Article 65 Decision: Draft Decision, paragraph 341.

"Services" under the basis of Article 6(1)(f) GDPR, especially regarding data subjects under the age of majority.

65. WhatsApp IE further relies on the legitimate interest to "secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products". It therefore "share[s] information with the Facebook Companies to promote safety and security" [171]. As is the case with the above example, the data subject has no information about the specific processing operation which would enable a data subject to properly exercise his or her data subject rights [172].

66. In conclusion, the EDPB considers that the finding of the IE SA in the Draft Decision that WhatsApp IE has complied, in full, with the requirements of Article 13(1)(d) GDPR does not correspond to the information that WhatsApp IE has provided to the data subjects, as stated in the relevant objections raised by the CSAs. The EDPB instructs the IE SA to alter its finding concerning the absence of an infringement of Article 13(1)(d) GDPR and to include such infringement in its final decision on the basis of the shortcomings identified by the EDPB."

416. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision **finds that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(d).**

Assessment: Article 13(1)(e) – the Recipients or Categories of Recipient

Required Information and WhatsApp's Response to Investigator's Questions

417. Article 13(1)(e) requires a data controller to provide the data subject with information as to "the recipients or categories of recipients of the personal data, if any."

418. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

> *"[WhatsApp] identifies the recipients and potential recipients of a user's personal data in the following sections of the Privacy Policy: 'Information You And We Share', 'How We Work With Other Facebook Companies' and 'Assignment, Change Of Control, And Transfer'."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

419. The Investigator considered the extent to which WhatsApp complied with its obligations under this heading by reference to **Proposed Finding 10**. She proposed a finding, under this heading, that the information provided by WhatsApp was not sufficiently clear to satisfy the requirement of transparency pursuant to Article 12(1) "due to insufficient detail being provided to the data subject about the circumstances in which their personal data would be transferred and to whom such transfers are made." The Investigator noted, in this regard, that the seven listed purposes for which WhatsApp shares personal data with "third-party service providers" was "wide-ranging" yet WhatsApp had not provided a definition of who might comprise this category of recipients.

[171] Footnote from the Article 65 Decision: Draft Decision, paragraph 341.
[172] Footnote from the Article 65 Decision: See "Good Practice Examples", Transparency Guidelines, page 9.

420. WhatsApp rejected this proposed finding. It submitted[173] that:

> *"Under the "Information You and We Share" section of the Privacy Policy, WhatsApp separately identifies "third party service providers" as a category of recipients. WhatsApp details, in clear and plain language and in a concise manner, the types of processing activities that these service providers undertake for WhatsApp as well as giving assurances as to the contractual obligations on those providers. Examples ensure that users can understand how these companies provide services to and on behalf of WhatsApp, whilst avoiding technical or complex terms like data processor or data processing agreement.*

421. The Investigator was unconvinced by WhatsApp's submissions, in this regard, and confirmed her view, by way of Conclusion 10, that the information provided by WhatsApp failed to satisfy the requirements of Articles 13(1)(e) and 12(1) of the GDPR.

Assessment of Decision-Maker: What information has been provided?

422. The sections of the Privacy Policy identified by WhatsApp contain the following relevant information:

> *"Information You And We Share*
> *… we share your information to help us operate, provide, improve, understand, customize, support, and market our Services.*
> - ***…***
> - ***Businesses On WhatsApp.*** *We help businesses who use WhatsApp measure the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services.*
> - ***Third-Party Service Providers.*** *We work with third-party service providers and the Facebook Companies to help us operate, provide, improve, understand, customize, support, and market our Services. ….*
> - ***… .*** *"*

423. Also:

> *"**How We Work With Other Facebook Companies***
> *We are part of the Facebook Companies. As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies. ….*
> *Learn More about how WhatsApp works with the Facebook Companies."*

424. And, finally:

> *"**Assignment, Change of Control, And Transfer***
> *All of our rights and obligations under our Privacy Policy are freely assignable by us to any of our affiliates, in connection with a merger, acquisition, restructuring, or sale of assets, or by operation of law or otherwise, and we may transfer your information to any of our affiliates, successor entities, or new owner."*

[173] The Inquiry Submissions, paragraph 12.2

Assessment of Decision-Maker: How has the information been provided?

425. The information described above has been provided in three different sections of the Privacy Policy. The links embedded in the text quoted above relate to the following additional text/information:

    a. The link embedded the "Facebook Companies" text, as listed above, links the user to an article entitled "The Facebook Companies" on Facebook's website. That contains further links to three other "articles" on Facebook's website (each linking back to the others).

    b. The link embedded in the "Learn More" text, at the end of the "How We Work With Other Facebook Companies" section, links the user to a FAQ located elsewhere on the WhatsApp website entitled "How we work with the Facebook Companies"[174] (that FAQ contains further embedded links and some of the text that can be accessed by these links contain further links to further information).

Finding: Article 13(1)(e) – the Recipients or Categories of Recipient

Quality of information provided

426. The obligation arising, under this heading, is to provide information to the data subject in relation to the recipients or categories of recipient of the data. The Article 29 Working Party expressed the view, in the Transparency Guidelines[175], that the information required to be provided under this heading is as follows:

> *"The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data.* ***If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients****."* [emphasis added]

427. I agree with the view expressed by the Working Party that the information provided (where it has been provided by reference to categories of recipient) should be as specific as possible so as to provide the data subject with meaningful information under this heading. Accordingly, I consider that, in order to achieve compliance with this requirement, WhatsApp must provide the following information to users, and in a way that enables the user to quickly and easily locate and identify:

    a. The categories of third-party service providers that will receive his/her personal data as part of the provision of any required services to WhatsApp, including a brief description of the services in question in a manner that enables the user to understand why his/her personal data is being transferred and why/for what purpose(s) it is being transferred; and

    b. The categories of third-party that will receive his/her personal data as part of the provision of services, by WhatsApp, to the parties concerned, including a brief description of the

[174] Available at https://faq.whatsapp.com/general/26000112/?eea=1 (the "**Facebook FAQ**")
[175] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")

services in question in a manner that enables the user to understand why his/her personal data is being transferred and why/for what purpose(s) it is being transferred.

428. Further, I am of the view that the information should be provided such that the user should be able to identify what categories of his/her personal data will be received by the identified categories of recipient. As discussed in the "Preliminary Issue" section of the Article 13(1)(c) assessment, the quality of information that is provided to a data subject directly impacts on the effectiveness of that data subject's rights. Unless the user can identify what categories of his/her personal data are transferred to any identified recipients and why it is being transferred, the user is deprived of the information required to firstly understand the true consequences of the transfer for the data subject, as emphasised by the Transparency Guidelines[176], and, secondly, assess whether or not he/she might wish to consider exercising one or more of his/her rights.

429. With the exception of the Facebook FAQ, the information provided in relation to the categories of recipient does not enable the user to understand what categories of personal data will be sent to which category of recipient, nor to understand in a meaningful way why such transfers are being carried out and, therefore, the consequences for the data subject. The information furnished, in relation to the categories of recipient is insufficiently detailed so as to be meaningful to the user. For the avoidance of doubt, I will address the quality of information provided by the Facebook FAQ, in relation to the Facebook Companies, under Part 3 of this Decision.

Manner in which information has been provided

430. As before, I consider that there are deficiencies in the manner in which information has been provided under this heading. Again, the data subject is required to pursue further information by way of links to further texts, which themselves contain further links to additional texts. The information to be provided, under this heading, is not complex and neither is the information that WhatsApp has available to provide, under this heading. It seems to me that elements of this information are already scattered throughout the Terms of Service, Privacy Policy, Legal Basis Notice and linked articles/documents/FAQs. In the circumstances, it should be a straightforward task to collate this information and present it to the data subject in a clear and concise format.

431. Finally, I note that the "Assignment, Change of Control and Transfer" clause appears to have been included both in the Privacy Policy and Terms of Service. It seems to me that, from the perspective of the function of the Privacy Policy, this clause serves no function and is more appropriately included in the Terms of Service. If this clause is to remain in the Privacy Policy, I consider that it should be tempered by the addition of a statement to confirm that the data subject will be notified of any such changes in advance (as confirmed by the "Updates To Our Policy" clause). Otherwise, and to be absolutely clear, the clause itself, as currently drafted, does not, in my view, communicate information of the quality required by Article 13(1)(e).

432. For the reasons set out above, the Preliminary Draft included a proposed finding that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(e) and Article 12(1).

<u>WhatsApp's Response to Proposed Finding and Assessment of Decision-Maker</u>

[176] Transparency Guidelines, paragraph 10

433. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that:

> *"for the same reasons as set out above in relation to Article 13(1)(c) GDPR, WhatsApp disagrees with the Commission's analysis that granular information should be provided to users identifying the categories of personal data which will be received by the identified categories of recipients. This requirement departs from the clear language of the GDPR and is supplemental to the information points outlined by the Transparency Guidelines on Article 13(1)(e)[177]."*

434. It is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters. I acknowledge, however, that WhatsApp has decided[178] to relocate the "Assignment, Change of Control and Transfer" section to the Terms of Service, in light of the views I expressed in the Preliminary Draft. **Accordingly, for the reasons already set out above, I find that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(e) and Article 12(1).**

Assessment: Article 13(1)(f) – Transfers of personal data to a third country

Required Information and WhatsApp's Response to Investigator's Questions

435. Article 13(1)(f) requires the data controller, "where applicable", to inform the data subject "that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the [European] Commission, or in the case of transfers referred to in Article 46 or 47, or the second paragraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available."

436. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

> *"[WhatsApp] identifies the fact that it intends to transfer personal data to a third country or international organisation in the 'Our Global Operations' section of the Privacy Policy."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

437. The Investigator considered the extent to which WhatsApp complied with its obligations under this heading by reference to **Proposed Finding 11**. She expressed the view that the information provided was not sufficiently clear to satisfy the requirements of Article 12(1) of the GDPR. Further, the use of conditional language ("may"), in the context of possible reliance on adequacy decisions, was, in the Investigator's view, contrary to the requirement for a data controller to provide clear and transparent information to data subjects.

[177] The Preliminary Draft Submissions, paragraph 8.3
[178] The Preliminary Draft Submissions, paragraph 8.5

438. Further, the Investigator was concerned that the inclusion of a link that brings the user to information hosted on Facebook's website risked confusing the data subject as to the identity of the data controller with regard to third country transfers.

439. Accordingly, the Investigator proposed a finding that the information provided, under this heading, did not provide the minimum level of information required by Article 13(1)(f). Further, the information that had been provided was insufficiently clear to satisfy the requirements of Article 12(1) of the GDPR.

440. WhatsApp rejected this proposed finding. It submitted[179] that:

> *"On a proper analysis, the drafting of [the "Our Global Operations"] section of WhatsApp's Privacy Policy represents quite a meticulous implementation of the detailed requirements of this part of Article 13(1)".*

441. WhatsApp further submitted[180] that:

> *"The Draft Report takes the view that WhatsApp must be explicit in respect of each recipient and each country to which it transfers personal data. Not only is this not required by the GDPR … it is also impractical and would require a controller operating a service such as WhatsApp to continuously update its privacy notice in the (likely frequent) event it engaged a new service provider based in a different jurisdiction outside the EEA. There is simply no statutory basis for this interpretation of the GDPR and, in any event, such an approach would result in excessive and confusing information for users. … Moreover, the fact that WhatsApp relies on safeguards to transfer personal data of its EU users instead of relying entirely on derogations, and communicates this to its users, provides a significant level of protection. The further level of specificity described in the Draft Report is simply not a legal requirement."*

442. The Investigator was not swayed by WhatsApp's submissions, in this regard, and confirmed her view, by way of Conclusion 11, that WhatsApp failed to discharge its obligations pursuant to Article 13(1)(f) in circumstances where it failed to provide the minimum level of information required.

Assessment of Decision-Maker: What information has been provided?

443. The "Our Global Operations" section of the Privacy Policy includes the following information:

> *"**Our Global Operations***
> *… Information controlled by WhatsApp 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 Privacy Policy. … We utilize standard contract clauses approved by the European Commission, and may rely on the European Commission's adequacy decisions about certain countries, as applicable, for data transfers from the European Economic Area to the United States and other countries.*
> *…."*

[179] The Inquiry Submissions, paragraph 13.2
[180] The Inquiry Submissions, paragraph 13.3

Assessment of Decision-Maker: How has the information been provided?

444. The information has been provided in the Privacy Policy, as outlined above. The text contains two embedded links, as follows:

    a. The "standard contract clauses" link brings the user directly to an "article" hosted on Facebook's website, entitled "What is a standard contract clause?". There is a further link within that "article" that links the user to the relevant landing page (providing information on standard contractual clauses generally) on the European Commission's website;

    b. The "adequacy decisions" link brings the user directly to the relevant landing page (providing information on adequacy decisions generally) on the European Commission's website.

Finding: Article 13(1)(f) – Transfers of personal data to a third country

445. Identifying, firstly, the information required to be provided under this heading, Article 13(1)(f) specifies the following information:

    a. Where applicable, the fact that the controller intends to transfer personal data to a third country … and

    b. The existence or absence of an adequacy decision … , or

    c. … reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

446. Considering, firstly, the information required to be provided by Article 13(1)(f), I note the requirement for the controller to inform the data subject as to "the existence or absence" of an adequacy decision. This language goes beyond a requirement for the data controller to identify "if" or "whether" an adequacy decision exists in relation to the proposed country of transfer and instead requires a controller to provide definitive information such that the data subject is informed either (i) that the transfer is subject to an adequacy decision; or (ii) that the transfer is not subject to an adequacy decision.

447. WhatsApp, however, has simply advised that it "may" rely on adequacy decisions, "if applicable". This does not appear to be sufficient for the purpose of Article 13(1)(f). Neither is it sufficiently transparent for the purpose of Article 12(1) as to whether adequacy decisions are relied on.

448. Considering what additional information might be required to be provided, I note that, in the case of a transfer which is not the subject of an adequacy decision, the data controller must provide "reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available." This information requirement is quite specific; in effect it enables the data subject to access, if he/she so wishes, detailed information about the safeguards being used to protect his/her personal data. That being the case, it would not make sense if the data subject were not entitled to access information of similar quality in a case where his/her data is being transferred in reliance on an adequacy decision.

449. On the basis of the above, it seems to me that, while Article 13(1)(f) does not expressly require a data controller to identify the country of transfer, this information should be provided if it enables the data

subject to receive transparent and meaningful information as to those transfers taking place pursuant to an adequacy decision. If a controller does not want to provide this specific information, it must find another way to enable the data subject to access information in relation to the (specific) adequacy decision supporting the transfer such that he/she is enabled to access information of similar quality to that which he/she is entitled to receive if the transfer is supported by other safeguards.

450. I note, in this regard, that the Working Party, in the Transparency Guidelines[181], expressed the view that Article 13(1)(f) requires the provision of information as to:

> *"The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45 / binding corporate rules under Article 47 / standard data protection clauses under Article 46.2 / derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used.* ***In accordance with the principles of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects****; this will generally mean that the third countries be named."* [emphasis added]

451. As discussed in the "Preliminary Issue" section of the Article 13(1)(c) assessment, the quality of information that is provided to a data subject directly impacts on the effectiveness of that data subject's rights. Accordingly, I am of the view that, in order to comply with Articles 13(1)(f) and 12(1), the data controller must provide the required information in such a way that enables the data subject to identify the categories of personal data that will be transferred. This knowledge is particularly significant in circumstances where the conditions attaching to the transfer (as recorded in the adequacy decision or other suitable safeguard) may specify the categories of personal data that may be transferred in reliance on the decision/safeguard in question. Without confirmation of the precise categories of data being transferred, the data subject is deprived of the information he/she needs to consider whether or not he/she might wish to exercise his/her rights.

452. The information provided by WhatsApp, under this heading, does not appear to satisfy the requirements of Articles 13(1)(f) and 12(1) in circumstances where it does not:

a. provide the required information by reference to specified categories of data;

b. definitely identify whether or not an adequacy decision exists to support the transfer of a specified category of data such as to satisfy the requirement for transparency given the residual lack of clarity about whether (and, if so, what) adequacy decisions are relied on;

c. enable the data subject to access more information, in a meaningful way, about the adequacy decision(s) being relied on such as to satisfy the requirement for transparency given the residual lack of clarity about whether (and, if so, what) adequacy decisions are relied on. I note, in this regard, that a link has simply been provided to the relevant page on the European Commission's website. While this is better than nothing, a user is unable to identify which adequacy decision is being relied upon, such that he/she can access further information.

[181] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")

453. To be clear, it is not sufficient to simply provide a link to a generic European Commission webpage. The Transparency Guidelines make it clear that the data subject should be able to access (or obtain access, if access is not directly provided) to the particular document being relied upon, i.e. in this case, the specific set of standard contractual clauses or specific adequacy decision.

454. For the sake of completeness (and as already observed elsewhere in this Decision), I am further not in favour of the existing position whereby the data subject is invited to access further information about standard contractual clauses on Facebook's website. This is particularly the case where the information provided is so minimal that there is no (apparent) reason why it could not be provided on WhatsApp's website.

455. For the reasons set out above, the Preliminary Draft proposed a finding that WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1).

WhatsApp's Response to Proposed Finding and Assessment of Decision-Maker

456. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting firstly that my view that controllers must provide information on the categories of personal data which will be transferred is "without support in the text of the GDPR itself[182]". It secondly noted that the Preliminary Draft "*is the first time detailed interpretative guidance has been given on the implementation of [Article] 13(1)(f) by the Commission, and in particular how to implement the obligation in respect of providing additional information to data subjects*[183]." WhatsApp further noted "two key points", as follows:

> *"First, the mechanism relied on by WhatsApp depends on the country to which data will be transferred so, in the context of a service available in most parts of the world, WhatsApp considers that language such as "many" [sic] and "as applicable" [sic] is appropriate. Second, WhatsApp enables data subjects to access more information about adequacy decisions (and standard contractual clauses) by providing a link to the European Commission website. It also, in accordance with Article 13(1)(f) GDPR, enables users to access a copy of the standard contractual clauses relied on[184]."*

457. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. That assessment already explains my position on the matters raised by WhatsApp in the Preliminary Draft Submissions. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters. My assessment of WhatsApp's submission that this is the first time that "detailed interpretive guidance" has been provided in relation to the interpretation of Article 13(1)(f) is recorded as part of my assessment of WhatsApp's Submissions of General Application, above**. Accordingly, I find that WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1)**.

[182] The Preliminary Draft Submissions, paragraph 9.3
[183] The Preliminary Draft Submissions, paragraph 9.4
[184] The Preliminary Draft Submissions, paragraph 9.5

Assessment: Article 13(2)(a) – Retention Criteria/Retention Periods

Required Information and WhatsApp's Response to Investigator's Questions

458. Article 13(2)(a) requires the data controller to provide the data subject with information in relation to "*the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period*."

459. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

> *"[WhatsApp] explains the period for which personal data will be stored and how this is determined in the 'Managing and Deleting Your Information' section of the Privacy Policy."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

460. The Investigator considered the extent to which WhatsApp complies with its obligations under this heading by reference to **Proposed Finding 12**. She expressed the view that the information provided by WhatsApp, in this regard, was "generic". Further, the language used was "wide-ranging" in that there was no indication as to the circumstances that might constitute "operational retention needs".

461. Accordingly, the Investigator proposed a finding that WhatsApp failed to comply with the requirements of Article 13(2)(a).

462. WhatsApp rejected this proposed finding. It submitted[185] that this information was "clearly" explained to users in the Privacy Policy. Further, it submitted[186] that:

> *"Where possible, WhatsApp also provides users with additional contextual information on retention. For example the "Deleting your account" FAQ also sets out the process which follows deletion of an account, in that it "may take up to 90 days to delete data stored in backup systems" and that "personal information shared with the other Facebook Companies will also be deleted".*
>
> *The reality for WhatsApp (and the vast majority of online companies of any significant size) is that it is not in a position to inform a data subject at the time their personal data is collected of the specific time period for which it will be stored, in a way that would accord with the principles of Article 12(1) GDPR (i.e. ensuring the notice is concise, transparent, intelligible and in clear and plain language). This is because there are too many variables to do this at scale in a concise and accessible way via a privacy policy. This is precisely why Article 13(2)(a) GDPR does not require controllers to provide specific retention periods to data subjects where it is not possible to do so."*

463. The Investigator was unconvinced by WhatsApp's submissions and noted that she had not suggested that precise retention periods were required for all personal data. She confirmed, by way of Conclusion 12, that she remained of the view that WhatsApp failed to comply with its obligations pursuant to Article 13(2)(a) in circumstances where it failed to furnish sufficient detail in relation to the retention periods, or the criteria used to determine such retention periods, in operation in relation to the personal data it processes.

[185] The Inquiry Submissions, paragraph 14.1
[186] The Inquiry Submissions, paragraphs 14.2 and 14.3

Assessment of Decision-Maker: What information has been provided?

464. The identified section of the Privacy Policy provides as follows:

> *"**Managing And Deleting Your Information***
> *We store information until it is no longer necessary to provide our services, or until your account is deleted, whichever comes first. This is a case-by-case determination that depends on things like the nature of the information, why it is collected and processed, and relevant legal or operational retention needs.*
>
> *If you would like to manage, change, limit, or delete your information, we allow you to do that through the following tools:*
> *…*
> - ***Deleting Your WhatsApp Account.** You may delete your WhatsApp account at any time (including if you want to revoke your consent to our use of your information) using our in-app delete my account feature. When you delete your WhatsApp account, your undelivered messages are deleted from our servers as well as any of your other information we no longer need to operate and provide our Services. Be mindful that if you only delete our Services from your device without using our in-app delete my account feature, your information may be stored with us for a longer period. Please remember that when you delete your account, it does not affect the information other users have relating to you, such as their copy of the messages you sent them."*

465. I note, however, that further information has been provided in the "How to Delete Your Account" FAQ[187]. While this assessment has been carried out by reference to the Privacy Policy and any linked texts/documents/notices, WhatsApp, as part of its Inquiry Submissions, made specific reference this FAQ in support of its approach under this heading. Accordingly, I have reviewed this document as part of my assessment. I note that this document states:

> *"**How to delete your account***
> *You can delete your account from within WhatsApp. Deleting your account is an irreversible process, which we cannot reverse even if you perform it by accident.*
> *…*
> ***Deleting your account will:***
> - *Delete your account info and profile photo.*
> - *Delete you from all WhatsApp groups.*
> - *Delete your WhatsApp message history on your phone and your iCloud backup.*
>
> ***If you delete your account:***
> - *You can't regain access to your account.*
> - *It may take up to 90 days from the beginning of the deletion process to delete your WhatsApp information. Copies of your information may also remain after the 90 days in the backup storage that we use to recover in the event of a disaster, software error, or other data loss event. Your information isn't available to you on WhatsApp during this time.*
> - *It doesn't affect the information other users have relating to you, such as their copy of the messages you sent them.*
> - *Copies of some materials such as log records may remain in our database but are disassociated from personal identifiers.*

[187] Available at https://faq.whatsapp.com/en/general/28030012/ (the ""**How to Delete Your Account" FAQ**")

- *We may also keep your information for things like legal issues, terms violations, or harm prevention efforts.*
- *Please refer to the Law and Protection section of our Privacy Policy for more information.*
- *Your personal information shared with other Facebook Companies will also be deleted."*

466. The "Law And Protection" section of the Privacy Policy (accessible via the link in the "How to Delete Your Account" FAQ) provides that:

> *"**Law And Protection***
> *We collect, use, **preserve**, and share your information if we have a good-faith belief that it is reasonably necessary to: (a) respond pursuant to applicable law or regulations, to legal process, or to government requests; (b) enforce our Terms and any other applicable terms and policies, including for investigations of potential violations; (c) detect, investigate, prevent, and address fraud and other illegal activity, security, or technical issues; or (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook Companies, or others, including to prevent death or imminent bodily harm."* [emphasis added]

Assessment of Decision-Maker: How has the information been provided?

467. The information has been provided primarily by the "Managing And Deleting Your Information" section of the Privacy Policy. While the information provided by this text is simple and uncomplicated, it does not contain any reference to the possible preservation of data in the circumstances described in the "Law And Protection" section. Neither does it reference the retention of "information" or "materials", as described in the "How to Delete Your Account" FAQ[188].

Finding: Article 13(2)(a) – Retention Criteria/Retention Periods

468. The Working Party, in its Transparency Guidelines[189], expressed the view that:

> *"[The requirement to provide information as to the period of retention] is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e).*
>
> *The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods."*

469. I agree with the views expressed above and note that, again, what is required by Article 13(2)(a) is "meaningful" information. The information provided by WhatsApp, under this heading, is minimal. While a data subject would expect his/her personal data to be processed during the time while he/she is using the Services, he/she might not expect any processing to continue once he/she has deleted

[188] Available at https://faq.whatsapp.com/en/general/28030012/ (the ""**How to Delete Your Account" FAQ**")
[189] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")

his/her account. This is particularly the case where the "Managing and Deleting Your Information" section informs the user that WhatsApp stores information "until it is no longer necessary to provide our Services or until your account is deleted, **whichever comes first**" [emphasis added]. This is somewhat misleading in that it gives the impression that, if the user deletes his/her account, WhatsApp will no longer process his/her data.

470. Further, in relation to the variables that will determine the processing of data where the user has not deleted his/her account, WhatsApp has simply indicated that the period of post-deletion retention would be a case-by-case determination that depends on things like:

    a. The nature of the information;
    b. Why the information was collected and processed; and
    c. Relevant legal or operational retention needs.

471. This information does not assist the data subject to understand the basis for any retention of data because the significance of each criterion has not been clarified. WhatsApp should be able to provide practical examples of the how each of the above criteria impact on the period of retention so as to demonstrate accountability for compliance with the storage limitation principle.

472. Further, I note the additional information that has been provided in the "How to Delete Your Account" FAQ[190]. This clearly suggests that, notwithstanding the fact that a user may have deleted his/her account:

    a. Copies of the user's information may remain in WhatsApp's backup storage (but will not be available to the user during this time).

    b. Copies of some materials such as log records may remain in WhatsApp's database but are disassociated from personal identifiers.

    c. The user's information may be retained "for things like legal issues, terms violations, or harm prevention efforts" and for the purposes identified in the "Law And Protection" section of the Privacy Policy.

473. The above is most concerning given that the user is led to believe, by the clear statement, in the "Managing And Deleting Your Information" that WhatsApp "allows" a user to delete his/her information by way of the "in-app delete my account feature". Leaving aside the lack of clarity as to how WhatsApp will determine that it is necessary to "preserve" a user's information for any of the purposes set out in the "Law And Protection" section and the possibility that some data will be retained on back-up servers, the "How to Delete Your Account" FAQ[191] suggests that log records (and possibly other such records) will be retained in WhatsApp's database. No information has been provided in relation to how such records "are dissociated from personal identifiers". It is further concerning that this information has not been incorporated into the Privacy Policy (by way of link or otherwise), thus leaving it to chance as to whether a user will discover it. I note, in this regard, that the only reason I have this information is because WhatsApp included it by way of a footnote in its

[190] Available at https://faq.whatsapp.com/en/general/28030012/ (the ""**How to Delete Your Account" FAQ**")
[191] Available at https://faq.whatsapp.com/en/general/28030012/ (the ""**How to Delete Your Account" FAQ**")

Inquiry Submissions[192]; had it not been drawn to my attention, I would not have known of its existence.

474. Accordingly, I proposed a finding, in the Preliminary Draft, that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(a) in circumstances where:

a. No meaningful information has been provided in relation to the criteria that will be used to determine if, and for how long, a user's personal data will be retained following the deletion of his/her account;

b. Key information concerning the fact that certain information ("materials such as log records") will be retained, even after deletion, has not been incorporated into the Privacy Policy; and

c. Key information to explain how such retained records (i.e. those "materials such as log records") are "disassociated from personal identifiers" has not been incorporated into the Privacy Policy.

WhatsApp's Response to Proposed Finding and Assessment of Decision-Maker

475. WhatsApp, by way of the Preliminary Draft Submissions, maintained its position that, as far as it is concerned, it provides the information required by Article 13(2)(a). However, it further confirmed that, having reflected carefully on the Commission's views, it intends to make changes to the information that it provides to users under this heading[193].

476. In the absence of any substantive submissions from WhatsApp under this heading, my views remain as set out above. **Accordingly, I find that WhatsApp has failed to comply with its obligations under Article 13(2)(a).**

Assessment: Article 13(2)(b) – the existence of the data subject rights

Required Information and WhatsApp's Response to Investigator's Questions

477. Article 13(2)(b) requires the data controller to inform the data subject as to "the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability".

478. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

> *"[WhatsApp] explains the rights specified in Article 13(2)(b) in the Privacy Policy, under the section entitled 'How You Exercise Your Rights'."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

479. While the Investigator did not propose or confirm any particular finding or conclusion under this heading, she confirmed, in the Draft Report and Final Report, that she was satisfied that WhatsApp

[192] The Inquiry Submissions, paragraph 17.2 (and footnote number 77)
[193] The Preliminary Draft Submissions, paragraph 10.2

had complied with its obligations pursuant to Article 13(2)(b) in circumstances where clear information had been provided that could be easily understood and followed.

Assessment of Decision-Maker: What information has been provided?

480. The "How You Exercise Your Rights" section of the Privacy Policy provides the following information:

> *"… you have the right to access, rectify, port, and erase your information, as well as the right to restrict and object to certain processing of your information. This includes the right to object to our processing of your information for direct marketing and the right to object to our processing of your information where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party. … If we process your information based on our legitimate interests or those of a third party, or in the public interest, you can object to this processing, and we will cease processing your information, unless the processing is based on compelling legitimate grounds or is needed for legal reasons. … Where we use your information for direct marketing for our own Services, you can always object and opt out of future marketing messages using the unsubscribe link in such communications, or by using our in-app "Block" feature."*

Assessment of Decision-Maker: How has the information been provided?

481. The information has been provided in an appropriately named section of the Privacy Policy, as outlined above.

Finding: Article 13(2)(b) – the existence of the data subject rights

482. The information provided above is easy to locate and has been presented in a clear and concise manner. I further note that WhatsApp has specifically referenced the rights that may be exercised under the relevant sections of the Legal Basis Notice and has provided information as to how the data subject may go about exercising those rights. This represents a very thorough and comprehensive approach to this particular information requirement. **Accordingly, I find that WhatsApp has complied, in full, with its obligation to provide information pursuant to Article 13(2)(b).**

Assessment: Article 13(2)(c) – the existence of the right to withdraw consent

Required Information and WhatsApp's Response to Investigator's Questions

483. Article 13(2)(c) requires the data controller, in a case where the processing is based on the data subject's consent or explicit consent, to inform the data subject of "the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal."

484. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

> *"[WhatsApp] explains its approach to consent in the Privacy Policy and in the 'How We Process Your Information' notice."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

485. While the Investigator did not propose or confirm any particular finding or conclusion under this heading, she confirmed her view, in the Draft Report and Final Report, that the information provided

by WhatsApp, in this regard, was sufficiently clear to achieve compliance with the requirements of Article 13(2)(c).

Assessment of Decision-Maker: What information has been provided?

486. The relevant information provided, in the Privacy Policy, is as follows:

> *"**Managing And Deleting Your Information***
> *…*
> - ***Deleting Your WhatsApp Account.** You may delete your WhatsApp account at any time (including if you want to revoke your consent to our use of your information) using our in-app delete my account feature."*

487. In the section entitled "How The General Data Protection Regulation Applies To Our European Region Users", the use of consent as a legal basis for processing as identified as follows:

> *"We collect, use, and share the information we have as described above:*
> - *…*
> - *consistent with your consent, which you can revoke at any time"*

488. The Legal Basis Notice further provides, in the "Your Consent" section, that:

> "*When we process data you provide to us based on your consent, you have the right to withdraw your consent at any time and to port that data you provide to us, under the GDPR. To exercise your rights, visit your device-based settings, your in app-based settings like your in-app location control, and the How You Exercise Your Rights section of the Privacy Policy."*

Assessment of Decision-Maker: How has the information been provided?

489. As set out above, the relevant information has been provided in the Privacy Policy and Legal Basis Notice.

Finding: Article 13(2)(c) – the existence of the right to withdraw consent

490. While the statement in the "Your Consent" section of the Legal Basis Notice clearly references the right to withdraw consent, it does not include the full extent of information required by Article 13(2)(c) in that the qualifier "without affecting the lawfulness of processing based on consent before its withdrawal" has been omitted. This qualifier is important in that it firstly helps to manage the data subject's expectations and secondly helps to ensure that the data subject is adequately informed about the consequences of exercising this right.

491. Further, I note that:

    a. The "How You Exercise Your Rights" section does not include reference to the right to withdraw consent to processing or how a data subject might go about exercising this right. Given the title of this section, I am of the view that this is where the data subject is most likely to go to search for information about his/her rights. In the circumstances, reference to the right to withdraw consent should be included here.

b. The statement included in the "Managing and Deleting Your Information" section, as identified above, risks creating the impression that, in order to withdraw consent to consent-based processing, the data subject will have to delete his/her account (as opposed to simply adjusting his/her device-based settings).

492. The issues outlined above again arise as a result of a piecemeal approach to the provision of the required information. The effectiveness or otherwise of this approach is entirely dependent on which section the data subject visits first and whether or not he/she decides to look for further information in other locations. The information that is required to be given, under this heading, is not complex and, while WhatsApp has taken steps towards compliance, those steps are, in my view, rendered ineffective as a result of the scattering of slightly different information on the subject in three different areas of the Privacy Policy. As before, the issue here is the lack of a concise approach to the provision of the prescribed information.

493. For the reasons set out above, I proposed a finding, in the Preliminary Draft, that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1).

WhatsApp's Response to Proposed Finding and Assessment of Decision-Maker

494. By way of the Preliminary Draft Submissions, WhatsApp confirmed its disagreement with the above assessment, submitting that:

a. "*As a preliminary comment WhatsApp did not provide its views on compliance with Article 13(2)(c) GDPR in the Inquiry Submissions as the investigator found the information provided was sufficiently clear*[194]."

b. While WhatsApp would address the minor omission of the qualifying text, "*it is important to note that … the first column to the Annex to the Transparency Guidelines does not indicate this qualifier should be included and WhatsApp had followed this guidance when endeavouring to comply with this provision*[195]."

495. Having considered the above submissions, I firstly acknowledge that WhatsApp did not provide its views on compliance, under this heading, at the inquiry stage. I do not consider that WhatsApp has been disadvantaged or prejudiced in any way by this, however, given that it had the opportunity to put forward its case in response to the Investigator's initial questions and, again, in response to the Preliminary Draft. In relation to the absence of the qualifying wording from the Annex to the Transparency Guidelines, I note that the column in question is entitled "Required Information Type" [emphasis added] and that the contents of this column do not reflect, in each case, the precise wording of Article 13. I note, in any event, that the Transparency Guidelines do not take precedence over the clear language of Article 13(2)(c).

496. As before, it is clear that WhatsApp and I remain in disagreement as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp's

[194] The Preliminary Draft Submissions, paragraph 11.2
[195] The Preliminary Draft Submissions, paragraph 11.4

perspective on matters. I note, however, that WhatsApp will take account of my views[196], as regards the appropriate location for this particular information. **Accordingly, for the reasons already set out above, I find that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1).**

Assessment: Article 13(2)(d) – the right to lodge a complaint with a supervisory authority

Required Information and WhatsApp's Response to Investigator's Questions

497. Article 13(2)(d) requires the data controller to inform the data subject as to his/her right to "lodge a complaint with a supervisory authority".

498. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

> *"[WhatsApp] provides this information in the 'Contact Information' section of the Privacy Policy."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

499. The Investigator confirmed that she was satisfied that WhatsApp had complied with its obligations pursuant to Article 13(2)(d).

Assessment of Decision-Maker: What information has been provided?

500. The "Contact Information" of the Privacy Policy provides that:

> *"You have the right to lodge a complaint with WhatsApp Ireland's lead supervisory authority, the Irish Data Protection Commissioner, or your local supervisory authority."*

Assessment of Decision-Maker: How has the information been provided?

501. As set out above the relevant information has been included in the "Contact Information" section of the Privacy Policy. The language used is clear and concise.

Finding: Article 13(2)(d) – the right to lodge a complaint with a supervisory authority

502. While the information provided is clear and unequivocal, it has been presented in the "Contact Information" section of the Privacy Policy. The information required to be given, pursuant to Article 13(2)(d) is "the right to lodge a complaint with a supervisory authority". In the circumstances, it seems to me that it should be included, or at least cross-referenced, in the "How You Exercise Your Rights" section, given that this is likely the place where a data subject will first go to learn about his/her rights and how to access same.

503. In recognition of the fact that the required information has been delivered in such a clear and concise manner, **I find that WhatsApp has broadly complied with the obligation arising pursuant to Article 13(2)(d), subject to the direction that WhatsApp include reference to the existence of this right under the "How You Exercise Your Rights" section so as to ensure that the data subject is presented**

[196] The Preliminary Draft Submissions, paragraph 11.3

with the required information in a place where he/she might expect to find it. For the sake of completeness, the correct title of the Irish supervisory authority is the "Data Protection Commission".

504. I note that WhatsApp, by way of the Preliminary Draft Submissions, has confirmed[197] its intention to implement the change outlined above.

Article 13(2)(e) – whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

Required Information and WhatsApp's Response to Investigator's Questions

505. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

> *"[WhatsApp] identifies this information in the Privacy Policy and the 'How We Process Your Information' notice."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

506. The Investigator did not propose or confirm any finding or conclusion under this heading.

Assessment of Decision-Maker: What information has been provided?

507. The Privacy Policy, in the "Information We Collect" section states that:

> "*WhatsApp must receive or collect some information to operate, provide, improve, understand, customize, support, and market our Services … . The types of information we receive and collect depend on how you use our Services*."

508. The use of the word "must" denotes a mandatory requirement. In contrast, the use of the word "may", as used more generally within the "Information We Collect" section, indicates that the provision of the relevant information is not compulsory. The word "may" has been used, for example, in the context of the user's email address and other account information "such as a profile picture and about information".

509. Under the "Your Account Information" sub-heading, "may" is not used in conjunction with the provision of access to the phone numbers in the user's mobile address book. Under the "Your Connection" sub-heading, however, the word "may" is used in reference to the Contact Feature – "we **may** help you identify your contacts who also use WhatsApp" [emphasis added].

510. Under the heading "Automatically Collected Information", the word "may" is used in the context of location information collected "if" the user has chosen to share location with his/her contacts, etc. pursuant to WhatsApp's "location features".

511. The Legal Basis Notice (within the contractual necessity section) provides that:

[197] The Preliminary Draft Submissions, paragraph 12.1

> *"We'll use the data we have to provide these services; if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted."*

512. For the sake of completeness, the Terms of Service, in the "About Our Services" section, provides that:

> *"**Registration.** You must register for our Services using accurate information, provide your current mobile phone number, and, if you change it, update your mobile phone number using our in-app change number feature. … .*
>
> ***Address Book.** You provide us, all in accordance with applicable laws, the phone numbers of WhatsApp users and your other contacts in your mobile address book on a regular basis, including for both the users of our Services and your other contacts."*

Assessment of Decision-Maker: How has it been provided?

513. As set out above, the information provided has been included in various sections of the Privacy Policy, Legal Basis Notice and Terms of Service. The language used, however, does not clearly identify the data that must be provided or the consequences of failure to provide that data.

Finding: Article 13(2)(e) - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

514. Article 13(2)(e) requires the provision of the following information:

    a. Whether the provision of personal data is a statutory or contractual requirement,
    b. Or a requirement necessary to enter into a contract,
    c. As well as whether the data subject is obliged to provide the personal data
    d. And of the possible consequences of failure to provide such data

515. It stands to reason that WhatsApp needs to process a certain, minimum amount of personal data in order to provide the Service. The extent of the minimum required, however, is not clear from any of the text outlined above. Further, the (possible) consequences of failure to provide data are not clearly set out for the data subject. The only reference to such consequences is set out in the Legal Basis Notice, within the contractual necessity section, as follows:

    "… if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted."

516. This is further confusing in circumstances where processing is either necessary for the purpose of administering a contract or it is not.

517. In the circumstances set out above, the Composite Draft contained a recommendation that WhatsApp consider its position in relation to the extent to which it has incorporated the information prescribed by Article 13(2)(e) into its Privacy Policy (and Legal Basis Notice). I proposed no finding under this heading in circumstances where the extent to which WhatsApp complies with the requirements of Article 13(2)(e) does not appear to have been pursued by the Investigator (notwithstanding that it is covered by the scope of the within Inquiry, as set out in the Notice of Commencement). Thus, the

commentary and recommendation set out in the Composite Draft were provided on an *obiter dicta* basis and solely for the purpose of assisting WhatsApp to achieve compliance with its transparency obligations.

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

518. The German (Federal) SA raised an objection to the outcome recorded under this particular heading. The objection concerned the fact that the Composite Draft proposed a recommendation, rather than a finding, as regards the extent to which WhatsApp has complied with its obligations pursuant to Article 13(2)(e).

519. 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 objection, the Board determined[198] as follows:

> *209. "Regarding the objection on Article 13(2)(e) GDPR, the EDPB notes that the IE SA indeed makes an assessment of WhatsApp's Privacy Policy "Information We Collect section", the "contractual necessity section" and the "About Our Services" section. Inter alia, the IE SA - in the view of the EDPB, rightfully - concludes that "[...] the language used does not clearly identify the data that must be provided or the consequences of failure to provide that data" and that certain parts of the cited Privacy Policy sections were confusing [199].*
>
> *210. However, the IE SA does not make use of its corrective powers stipulated in Article 58(2) GDPR but (merely) recommends that "[...] WhatsApp consider its position in relation to the extent to which it has incorporated the information prescribed by Article 13(2)(e) into its Privacy Policy (and Legal Basis Notice)" [200]. According to the IE SA, the reason for this approach was that "[...] the requirements of Article 13(2)(e) GDPR does not appear to have been pursued by the Investigator (notwithstanding that it is covered by the scope of the within Inquiry, as set out in the Notice of Commencement)" [201].*
>
> *211. The EDPB welcomes the IE SA's initiative to provide WhatsApp IE with recommendations in order to provide data subjects with clearer and more transparent information concerning the processing of personal data at stake. Nonetheless, it has to be noted that, according to the IE SA, the Inquiry concerned "[...] the question of compliance or otherwise by WhatsApp Ireland Limited ("WhatsApp") with its obligations pursuant to Articles 12, 13 and 14 of the GDPR" [202] without excluding Article 13(2)(e) GDPR from the Inquiry.*
>
> *212. Furthermore, the EDPB stresses the importance of the information obligations as only full compliance with all aspects of Article 13 GDPR enables data subjects to be aware of, and verify, the lawfulness of the processing and to effectively exercise their rights as guaranteed by the GDPR.*
>
> *213. Additionally, the EDPB notes that the IE SA in the Draft Decision stated that while "[i]t stands to reason that WhatsApp needs to process a certain, minimum amount of personal data in order to provide the Service", "[t]he extent of the minimum required [...] is not clear" from*

[198] The Article 65 Decision, paragraphs 208 to 218 (inclusive)
[199] Footnote from the Article 65 Decision: Draft Decision, paragraphs 496 and 499.
[200] Footnote from the Article 65 Decision: Draft Decision, paragraph 500.
[201] Footnote from the Article 65 Decision: Draft Decision, paragraph 501.
[202] Footnote from the Article 65 Decision: Draft Decision, paragraph 1.

the Privacy Policy, nor are the possible consequences of the failure to provide data clearly set out, except for a reference within the section of the Legal Basis Notice dedicated to contractual necessity: "if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted" [203]. The IE SA found this to be "further confusing in circumstances where processing is either necessary for the purpose of administering a contract or it is not" [204].

214. Indeed, controllers should make sure to avoid any confusion as to what the applicable legal basis is. This is particularly relevant where the appropriate legal basis is Article 6(1)(b) GDPR and a contract regarding online services is entered into by data subjects. Depending on the circumstances, data subjects may erroneously get the impression that they are giving their consent in line with Article 6(1)(a) GDPR when signing a contract or accepting terms of service [205].

215. The EDPB takes note of the arguments put forward in WhatsApp IE's submissions concerning whether Article 13(2)(e) GDPR was infringed. WhatsApp IE disagreed that an infringement of this provision took place, first of all, because the language of Article 13(2) GDPR makes clear that the requirements listed in this provision inherently depend on context and are only mandatory to the extent "necessary to ensure fair and transparent processing" [206]. The EDPB recalls that, instead, "there is no difference between the status of the information to be provided under sub-articles 1 and 2 of Articles 13 and 14 GDPR respectively, as all of the information across these sub-articles is of equal importance and must be provided to the data subject" [207]. WhatsApp IE also argued that the information to be provided pursuant to Article 13(2)(e) GDPR was adequately provided in the privacy policy and user-facing information, as well as in the sign-up flow [208]. Nevertheless, it appears from the observations made by the IE SA, as well as from the sentence quoted above from the Legal Basis Notice that such information was not provided in a way that clearly allows the user to understand what is necessary and what consequences arise from the failure to provide certain information, nor the nature of the "optional features".

216. The EDPB sees no justification in excluding Article 13(2)(e) GDPR from the formal decision since the scope of the investigation inter alia covered compliance with Article 13 GDPR as such. The EDPB indeed considers that a stance of a SA where it displays that it will not exercise corrective powers impairs the position of data subjects to be fully aware of the processing at stake as a mere recommendation cannot be enforced and WhatsApp IE is not obliged to follow the view of the IE SA in this regard.

217. Furthermore, the EDPB considers that a finding of an infringement instead of a recommendation concerning Article 13(2)(e) GDPR does not undermine WhatsApp IE's right to be heard, and in any case there is no right that certain aspects are excluded from an investigation. As outlined above, the investigation covered, inter alia, compliance with Article 13 GDPR as such, meaning the finding relates to the same subject-matter and not a completely different provision or chapter of the GDPR. Apart from this and as mentioned above, WhatsApp

[203] Footnote from the Article 65 Decision: Draft Decision, paragraph 498.
[204] Footnote from the Article 65 Decision: Draft Decision, paragraph 499.
[205] Footnote from the Article 65 Decision: EDPB Guidelines 2/2019 *on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, version 2 adopted 8 October 2019, p. 20.
[206] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 17.6(A).
[207] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 23.
[208] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 17.6(B)-(E).

IE was given the opportunity to reflect on a potential finding of an infringement, clearly setting out its arguments, and took the stance that it had not infringed Article 13(2)(e) GDPR [209].

218. Therefore, in the view of the EDPB, it is a mere legal assessment whether the relevant sections of the Privacy Policy of WhatsApp are in compliance with the GDPR or not as the factual findings (the use of the Privacy Policy of WhatsApp) are undisputed in this context and are sufficient to reach a legal conclusion. Therefore, the EDPB instructs the LSA to include in its final decision a finding of an infringement of Article 13(2)(e) GDPR, which it deems necessary as it considers a mere recommendation to be insufficient to ensure effective enforcement of the GDPR against WhatsApp IE and to fully protect the rights of natural persons as stipulated in Article 8 of the Charter of Fundamental Rights of the EU."

520. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision **finds that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(e)**.

Article 13(2)(f) – the existence of automated decision-making, including profiling

Required Information and WhatsApp's Response to Investigator's Questions

521. Article 13(2)(f) requires the data controller to provide information to the data subject as to "the existence of automated decision-making, including profiling … and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

522. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

> *"[WhatsApp] does not engage in the automated decision making referenced in Articles 22(1) and 22(4) of the GDPR."*

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

523. The Investigator did not propose or confirm any finding or conclusion under this heading.

Outcome of Assessment

524. I note that WhatsApp confirmed, from the outset, that it does not engage in the activities covered by Article 13(2)(f). In the circumstances, I note that no obligation arises for WhatsApp to provide information to data subjects under this heading. Accordingly, it is not necessary for me to reach any finding on compliance in relation to this particular obligation.

Part 3: Transparency in the Context of any Sharing of User Personal Data between WhatsApp and the Facebook Companies

[209] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 17.6.

Introduction

525. Under this heading, I will consider the extent to which WhatsApp complies with its transparency obligations by reference to WhatsApp's relationship with the Facebook Companies and any sharing of user data in the context of that relationship (for completeness, it should be noted that the issue of transparency obligations arising in the context of the sharing of non-user data by WhatsApp with any of the Facebook Companies has already been dealt with in Part 1). The issues that I will consider under this heading correspond to the matters covered by Conclusion 15 of the Final Report.

The Inquiry Stage

526. In its Response to Investigator's Questions, WhatsApp provided the following information:

> *"16. Please outline WhatsApp's compliance with Articles 13 and 14 GDPR in relation to the information provided to data subjects regarding how WhatsApp works with other Facebook companies, as outlined in its Terms of Service and Privacy Policy, including WhatsApp's online FAQ resource. In answering this question, please make reference to the requirements set out in Article 12 GDPR, with particular regard to any differences that may be present between these documents, in the language used to describe its current or potential future arrangements.*
>
> *Please see [WhatsApp's] response to question 4 describing the information provided to users in compliance with Article 13 regarding how [WhatsApp] works with other Facebook companies, including in particular the "How We Work With Other Facebook Companies" section. In addition, further information is available to users who click on the "Learn more" link which brings users to a dedicated section of [WhatsApp's] FAQ titled "How we work with the Facebook Companies" (attached hereto as Appendix 3). [WhatsApp] demonstrated how it complies with Article 12(1) in relation to the communication of this information in our response to question 5.*
>
> *With respect to [WhatsApp's] compliance with Article 14 and corresponding Article 12(1) obligations, please see the responses to questions 9 and 10.*
>
> *[WhatsApp] ensures that the information referred to in the preceding two paragraphs describes how it processes personal data of its users, including in the context of working with other Facebook companies."*

<u>The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion</u>

527. By reference to Proposed Finding 15, the Investigator proposed a finding that WhatsApp's approach to transparency, under this heading, did not comply with the requirements set out in Articles 12(1), 13(1)(e) and 13(1)(f) of the GDPR. She formed this view on the basis that:

    a. In order for a data subject to understand the manner in which his/her personal data, which is processed by WhatsApp, interacts with other Facebook Companies, the data subject must navigate a number of linked but separate documents on both the WhatsApp and Facebook websites.

    b. The language used in some of the text provided is conditional, e.g. "we *may* share …" [emphasis added]. Further the text failed to sufficiently clarify what information may be shared between the companies.

c. The text failed to identify the category of data subject that was covered by the term "you". This left it unclear as to whether the sharing of data occurred in the context of users, or non-users or both.

d. Further, the diversion of the data subject to the Facebook website risked creating confusion in relation to the entity/entities covered by the term "we". In other words, the data subject could interpret the term "we" as meaning WhatsApp, Facebook or any and all of the Facebook Companies.

528. WhatsApp rejected the Investigator's proposed finding and submitted[210] that:

> *"The Draft Report seeks to give the impression that information on the relationship between WhatsApp and the Facebook Companies is opaque and difficult to discern from the Online Documents. The opposite is in fact the case. The Draft Report fails to mention that the fact WhatsApp may share information with other Facebook Companies is explained in the "Key Updates" summary page at the very top of the Online Documents. It also fails to mention that WhatsApp provides a suite of FAQs addressing a range of different issues relevant to WhatsApp's relationship with other Facebook Companies (depending on what a particular user is interested in understanding), all of which are designed to maximize transparency around WhatsApp's processing activities. Only one of these FAQs is referred to in the Draft Report – described as the "WhatsApp Website FAQ document"."*

529. WhatsApp further submitted that the Draft Report failed to have due regard to the clear statements that had been included in various pieces of text "as to what Facebook cannot do with WhatsApp user data".

530. The Investigator was unconvinced by WhatsApp's submissions and confirmed her view, by way of Conclusion 15, that WhatsApp was not compliant with the transparency requirements, as specifically set out in Articles 12(1), 13(1)(e) and 13(1)(f) of the GDPR in the context of the information provided, explaining how it works with the Facebook Companies.

The Decision-Making Stage

531. The issue for assessment is the extent to which WhatsApp complies with its transparency obligations, by providing meaningful information in relation to how it works with other Facebook companies.

532. In its Response to Investigator's Questions, WhatsApp indicated that it provides information to users in relation to how it works with other Facebook Companies by way of the Privacy Policy and related pages (including the Legal Basis Notice), with particular reference to the "How We Work With Other Facebook Companies" section of the Privacy Policy and the linked FAQ entitled "How we work with the Facebook Companies[211]" ("the **Facebook FAQ**"). WhatsApp furnished a copy of the Facebook FAQ by way of Appendix 3 to its Response to Investigator's Questions.

[210] The Inquiry Submissions, paragraph 17.2

[211] Available at https://faq.whatsapp.com/general/26000112/?eea=1 (the "**Facebook FAQ**")

533. For the sake of completeness, I included, in my assessment, any additional sources of information identified by WhatsApp in its Inquiry Submissions. Those additional sources are as follows:

a. The "**I have Questions" FAQ**[212]; and

b. The "**How to Delete Your Account" FAQ**[213]

Preliminary Issue: The Status of the "I have Questions" FAQ

534. Further to my review of the "I have Questions" FAQ, I observed that this was the only text that expressly referenced the possible sharing of personal data with "Facebook and the Facebook family" for objectives including the possible delivery of "better friend suggestions and more relevant ads on Facebook". This directly contradicted the clear statement (that has been included in three separate places) in the Facebook FAQ that:

"Facebook does not use your WhatsApp account information to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook."

535. I was very concerned about the suggestion that Facebook might use personal data in the manner outlined in the "I have Questions" FAQ and, accordingly, I directed WhatsApp to specifically respond to the following questions, as part of any responding submissions:

a. Whether or not Facebook and/or the "Facebook family" uses data provided to it by WhatsApp to improve Facebook product experiences, by way of "better friend suggestions and more relevant ads on Facebook" or otherwise; and

b. If not, why the information referenced above has been included and made available in the "I have Questions" FAQ.

WhatsApp's Response to Questions Posed and Outcome of Preliminary Issue

536. By way of the Preliminary Draft Submissions, WhatsApp answered the above questions as follows:

a. In response to the first question, WhatsApp confirmed that it "*has had technical controls in place since 2016 to support its ongoing commitment to the [Commission] that Facebook (or any company in the Facebook family) will not use European Region WhatsApp users' data provided to it by WhatsApp to improve Facebook product experiences, by way of better friend suggestions and more relevant ads on Facebook or otherwise*". WhatsApp further confirmed that "*as previously committed to the [Commission], in the event that WhatsApp makes a decision to share such data with Facebook for these purposes in the future, it will only do so after prior discussion with [the Commission][214]."*

b. In response to the second question, WhatsApp explained that the "I have Questions" FAQ was referenced in error in the Inquiry Submissions. WhatsApp clarified that this FAQ "*was never intended to apply to users in the European Region under the GDPR and was deprecated globally*

[212] Previously available at https://faq.whatsapp.com/en/general/28030012/ (the ""**I have Questions" FAQ"**)
[213] Available at https://faq.whatsapp.com/en/general/28030012/ (the ""**How to Delete Your Account" FAQ**")
[214] The Preliminary Draft Submissions, paragraph 13.2

in April 2018." The link was "*reactivated in October 2018 as it was embedded in a historic blogpost mentioned in a media interview*". It would have only been available, however, to individuals who had a direct link, such as from the historic blogpost. WhatsApp confirmed that the FAQ could not be viewed when browsing the WhatsApp website, nor could it be located via the search function on the website. Otherwise, the FAQ was not linked to any other user-facing content. WhatsApp confirmed that the FAQ was archived in May 2020 and is no longer accessible via the respective link[215].

537. WhatsApp provided further assurance of the position by advising that "*the Facebook Companies have recently introduced further measures via its enhanced group wide privacy program which encompass monitoring and verifying data uses and practices. As part of these further measures, a range of data processing activities across the Facebook Companies are being reviewed, which will include the controls around the processing of European Region WhatsApp users' data by Facebook, to further ensure commitments such as those [set out above] remain accurate*[216]."

538. As regards the confirmation / explanation provided by WhatsApp, above, I note that the "I have Questions FAQ" was referenced in error in the Inquiry Submissions and that this document was not, at the relevant time, generally available. Accordingly, I have removed any further reference to the "I have Questions" FAQ from the record of assessment set out below.

Approach to Assessment

539. Given that the focus of this assessment is the extent to which information has been provided in relation to how WhatsApp works with other Facebook Companies, I consider that the required information is likely to be captured by the requirement to provide specific information under Articles 13(1)(c), 13(1)(d) and 13(1)(e), as follows:

    a. Article 13(1)(c): the purposes of the processing for which the personal data are intended as well as the legal basis for the processing. As part of my assessment under this heading, I will also consider the extent to which the personal data that will be shared with the Facebook Companies has been identified to the user.

    b. Article 13(1)(d): where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party.

    c. Article 13(1)(e): the recipients or categories of recipients of the personal data, if any.

540. For the avoidance of doubt, I considered the extent to which WhatsApp complies with its transparency obligations, <u>generally</u>, in Part 2 of this Decision. The focus of the assessment for the purpose of this Part 3, however, is the extent to which WhatsApp complies with its transparency obligations <u>in the specific context of explaining</u> its relationship with the Facebook Companies (and any consequent sharing of data).

541. Further, while I will carry out separate assessments of the information that has been provided further to each of Articles 13(1)(c), 13(1)(d) and 13(1)(e), I will conclude my overall assessment with a single

[215] The Preliminary Draft Submissions, paragraphs 13.4 and 13.5
[216] The Preliminary Draft Submissions, paragraph 13.3

finding, confirming my views as to whether WhatsApp has complied with the obligations arising in each case.

542. As before, I propose to approach my assessment by reference to the questions:

a. What information has been provided? And

b. How has that information been provided?

What information has been provided?

543. A range of information is available at the various sources identified by WhatsApp. For ease of assessment, I have summarised the information provided, and the location at which it is to be found, by reference to the following headings:

a. **Notification** of the relationship with the Facebook Companies and consequent sharing of data;
b. **Why** data is shared between WhatsApp and the Facebook Companies;
c. **What** data is shared between WhatsApp and the Facebook Companies;
d. **Legal Basis** relied upon to ground processing; and
e. **Recipients** of the data.

544. Headings a. – d., above, are addressed in Table 1, below. Information concerning the identities of the various entities comprising the Facebook Companies is made available through Facebook's website. Accordingly, the information provided in relation to heading e. above is addressed in Table 2, below.

545. ***Table 1***

	Information Provided	***Where provided***
Notification of the relationship with the Facebook Companies and consequent sharing of data		
1.	WhatsApp is one of the Facebook Companies	Introduction section at top of the Page
2.	We are part of the Facebook Companies. As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies as described in WhatsApp's Privacy Policy.	"Our Services" section of Terms of Service
3.	We are part of the Facebook Companies. Our Privacy Policy ("Privacy Policy") helps explain our information (including message) practices, including the information we process to support our Services.	Introduction section of Privacy Policy
4.	We are part of the Facebook Companies. As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies.	"How We Work With Other Facebook Companies" section of Privacy Policy

5.	WhatsApp Ireland shares information globally, both internally within the Facebook Companies, and externally with our partners and with those you communicate around the world in accordance with this Privacy Policy.	"Our Global Operations" section of Privacy Policy
6.	**Third-Party Services.** … . If you use our Services with such third-party services or Facebook Company Products, we may receive information about you from them; for example, if you use the WhatsApp share button on a news service to share a news article with your WhatsApp contacts, groups, or broadcast lists on our Services, or if you choose to access our Services through a mobile carrier's or device provider's promotion of our Services.	"Information We Collect" section of Privacy Policy
Why data is shared between WhatsApp and the Facebook Companies		
7.	We use the information we receive from [the Facebook Companies] to help operate, provide, and improve our Services.	"Our Services" section of Terms of Service
8.	WhatsApp works and shares information with the other Facebook Companies to receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and to keep WhatsApp and the Facebook Companies safe and secure.	Introduction section at top of Page Also in the Facebook FAQ
9.	When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. Working together allows us to: • Provide you fast and reliable messaging and calls around the world and understand how our services and features are performing • Ensure safety and security across WhatsApp and the Facebook Company Products by removing spam accounts and combatting abusive activity • Connect your WhatsApp experience with Facebook Company Products. For example, you could share a link to a post from Facebook to a WhatsApp chat. • Enable you to communicate with businesses on WhatsApp. For example if you visit a business's Facebook page, you might see a button that lets you easily open a WhatsApp chat with them.	Introduction section at top of Page
10.	Today, Facebook does not use your WhatsApp account information to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook. Learn more about how WhatsApp works with the Facebook Companies. [Link provided to the Facebook FAQ]	Introduction section at top of Page Also in the Facebook FAQ (multiple times)

11.	**Third-Party Service Providers.** We work with third-party service providers and the Facebook Companies to help us operate, provide, improve, understand, customize, support, and market our Services. For example, we work with companies to distribute our apps, provide our infrastructure, delivery, and other systems, supply location, map, and places information, process payments, help us understand how people use our Services, market our Services, help you connect with businesses using our Services, conduct surveys and research for us, and help with customer service. These companies may provide us information about you in certain circumstances; for example, app stores may provide us reports to help us diagnose and fix service issues.	"Information We Collect" section of Privacy Policy
12.	We may provide you marketing for our Services and those of the Facebook Companies. Please see How You Exercise Your Rights for more information.	"How We Use Information" section of Privacy Policy
13.	**Third-Party Service Providers.** We work with third-party service providers and the Facebook Companies to help us operate, provide, improve, understand, customize, support, and market our Services. When we share information with third-party service providers and the Facebook Companies in this capacity, we require them to use your information on our behalf in accordance with our instructions and terms.	"Information You And We Share" section of Privacy Policy
14.	We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customize, support, and market our Services and their offerings. This includes helping improve infrastructure and delivery systems, understanding how our Services or theirs are used, helping us provide a way for you to connect with businesses, and securing systems. We also share information to fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products. … Learn More about how WhatsApp works with the Facebook Companies.	"How We Work With Other Facebook Companies" section of Privacy Policy
15.	We may collect, use, preserve, and share your information if we have a good-faith belief that it is reasonably necessary to: … (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook Companies, or others …	"Law And Protection" section of Privacy Policy
16.	Information controlled by WhatsApp 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 Privacy Policy. These data transfers are necessary to provide the Services set forth in our Terms and globally to operate and provide our Services to you. …	"Our Global Operations" section of Privacy Policy

17.	To receive services that will help WhatsApp improve and develop our business. ○ We share information with the Facebook Companies (and trusted third parties) as service providers. Service providers help companies like WhatsApp by providing infrastructure, technologies, systems, tools, information, and expertise to help us provide and improve the WhatsApp service for our users. ○ This enables us, for example, to analyze and understand how our Services are being used, and how it compares to usage across the Facebook Companies. By sharing information with the Facebook Companies, such as the phone number you verified when you signed up for WhatsApp and the last time your account was used, we may be able to work out whether or not a particular WhatsApp account belongs to someone who also uses another service in the Facebook Companies. This allows us to more accurately report information about our Services and to improve our Services. So, for example, we can then understand how people use WhatsApp services compared to their use of other apps or services in the Facebook Companies, which in turn helps WhatsApp to explore potential features or product improvements. We can also count how many unique users WhatsApp has, for example, by establishing which of our users do not use any other Facebook apps and how many unique users there are across the Facebook Companies. This will help WhatsApp more completely report the activity on our service, including to investors and regulators. ○ It also helps WhatsApp as we explore ways to build a sustainable business. For example, as we announced in 2016, we're exploring ways for people and businesses to communicate using WhatsApp, and this could include working with the Facebook Companies to help people find businesses they're interested in and communicate with via WhatsApp. In this way, Facebook could enable users to communicate via WhatsApp with businesses they find on Facebook. ○ When WhatsApp shares information with them in these ways, the Facebook Companies act as service providers, in order to help WhatsApp and our family of companies. When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions.	The Facebook FAQ
18.	To keep WhatsApp and other Facebook family services safe and secure. ○ We share information with the Facebook Companies, and vice versa, to help fight spam and abuse on our Services, help keep them secure, and promote safety and security on and off our Services. So if, for example, any member of the Facebook	The Facebook FAQ

	Companies discovers that someone is using its services for illegal purposes, it can disable their account and notify the other Facebook Companies so that they can also consider doing the same. In this way, we only share information for this purpose in relation to users that have first been identified as having violated our Terms of Service or threatened the safety or security of our users, about which other members of our family of companies should be warned. o To keep WhatsApp and other Facebook Companies' services safe and secure, we need to understand which accounts across the Facebook Companies relate to the same user, so we can take appropriate action when we identify a user who violates our Terms of Services or presents a safety or security threat to others.	
19.	We do not share data for improving Facebook products on Facebook and providing more relevant Facebook ad experiences. o Today, Facebook does not use your WhatsApp account information to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook. ...	The Facebook FAQ
20.	... we need to have the ability to share information for all of our users, if necessary, in order to be able to receive valuable services from the Facebook Companies and fulfill the important purposes described in our Privacy Policy and this article.	The Facebook FAQ
What data is shared between WhatsApp and the Facebook Companies		
21.	Nothing you share on WhatsApp, including your messages, photos, and account information, will be shared onto Facebook or any of our other family of apps for others to see, and nothing you post on those apps will be shared with WhatsApp for others to see, unless you choose to do so.	Introduction section at top of Page ALSO: the Facebook FAQ
22.	However, your WhatsApp messages will not be shared onto Facebook for others to see. In fact, Facebook will not use your WhatsApp messages for any purpose other than to assist us in operating and providing our Services.	"How We Work With Other Facebook Companies" section of Privacy Policy
23.	WhatsApp currently shares limited categories of information with the Facebook Companies. This consists of the phone number you verified when you signed up for WhatsApp, some of your device information (your device identifier, operating system version, app version, platform information, your mobile country code and network code, and flags to enable tracking of the update acceptance and control choices), and some of your usage information (when you last used WhatsApp and the date you first registered your account, and the types and frequency of your features usage). In all cases, the information is shared securely and is not shared outside the	The Facebook FAQ

	Facebook Companies. The shared information will also not be seen by other users of any of the other Facebook Company Products.	
24.	Importantly, WhatsApp does not share your WhatsApp contacts with Facebook or any other members of the Facebook Companies, and there are no plans to do so. WhatsApp also does not share your messages with Facebook. In addition, WhatsApp cannot read your messages because they are end-to-end encrypted by default when you and the people you message with use the latest version of our app. Only the people you message with can read your messages – not WhatsApp, Facebook, or anyone else.	The Facebook FAQ
25.	If you delete your account: ... Your personal information shared with other Facebook Companies will also be deleted.	The "How to Delete Your Account" FAQ
Legal Basis relied upon to ground processing		
26.	**To share information with the Facebook Companies to promote safety and security.** See our Privacy Policy under "How We Work with Other Facebook Companies" for more information. The legitimate interests we rely on for this processing are: To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products.	Legitimate Interests section of Legal Basis Notice

546. The information available, by way of the various links embedded in the text "Facebook Companies" and "Facebook Company Products", is as follows:

547. ***Table 2***

	Information Provided	***Where Found***
Recipients of the data		
1.	**The Facebook Companies** In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below, in accordance with their respective terms of service and privacy policies. We may share information about you within our family of companies to facilitate, support and integrate their activities and improve our services. For more information on the Facebook Companies' privacy practices and how they treat individuals' information, please visit the following links: • Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy) and Facebook Payments International Limited (https://www.facebook.com/payments_terms/EU_privacy).	"The Facebook Companies" (article on Facebook's website)

	• Onavo (http://www.onavo.com/privacy_policy). • Facebook Technologies, LLC and Facebook Technologies Ireland Limited (https://www.oculus.com/legal/privacy-policy/). • WhatsApp Inc. and WhatsApp Ireland Limited (http://www.whatsapp.com/legal/#Privacy). • CrowdTangle (https://www.crowdtangle.com/privacy). … **Related Articles** The Facebook Company Products [see text below] How can I switch back to Classic Facebook? Can I search for specific videos on the Facebook Watch TV app? How do I get to the Facebook mobile site (m.facebook.com)? What are the Facebook Products? [see text below]	
2.	**The Facebook Company Products** The Facebook Company Products are, together, the Facebook Products[1] and other products provided by the Facebook Companies that are subject to a separate, stand-alone terms of service and privacy policy, including the WhatsApp, Oculus, and CrowdTangle websites, products, or apps.	"The Facebook Company Products" (article on Facebook's website)
3.	**[1]What are the Facebook Products?** The Facebook Products include Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network, NPE Team apps and any other features, apps, technologies, software, products, or services offered by Facebook Inc. or Facebook Ireland Limited under our Data Policy. The Facebook Products also include Facebook Business Tools[2], which are tools used by website owners and publishers, app developers, business partners (including advertisers) and their customers to support business services and exchange information with Facebook, such as social plugins (like the "Like" or "Share" button) and our SDKs and APIs. Facebook Products does not include some Facebook-offered products or services that have their own separate privacy policies and terms of service – such as Workplace, Free Basics, and Messenger Kids.	"What are the Facebook Company Products" (article on Facebook's website)
4.	**[2]The Facebook Business Tools** The Facebook Business Tools are technologies offered by Facebook Inc. and Facebook Ireland Limited that help website owners and	"Facebook Business Tools" (article on

	publishers, app developers, and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who use or might be interested in their products and services. These Tools include APIs and SDKs, the Facebook Pixel, Facebook social plugins, such as the Like and Share buttons, Facebook Login and Account Kit, and other Platform integrations, as well as other plugins, code, specifications, documentation, technology and services.	Facebook's website)
5.	**Facebook Cookie Banner** To help personalize content, tailor and measure ads, and provide a safer experience, we use cookies. By clicking or navigating the site, you agree to allow our collection of information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.	Facebook's Cookie Banner (presented once the user accesses the website via the links provided)

How has that information been provided?

548. As is evident from the above, the information has been provided in various locations, as follows:

a. Introduction section at top of the Page
b. "Our Services" section of the Terms of Service
c. Introduction section at top of Privacy Policy
d. "How We Work With Other Facebook Companies" section of Privacy Policy
e. "Our Global Operations" section of Privacy Policy
f. "Information We Collect" section of Privacy Policy
g. The Facebook FAQ
h. "How We Use Information" section of Privacy Policy
i. "Information You And We Share" section of Privacy Policy
j. "Law And Protection" section of Privacy Policy
k. Legal Basis Notice (Legitimate Interests Section)
l. The "How to Delete Your Account" FAQ

549. In addition to the above, the user is invited to find out more information by way of links to two different "articles" hosted on Facebook's website. Once the user accesses that website, he/she is immediately presented with a cookie banner. With the linked articles, there are further links provided to other "articles". In total, the user is presented with information in five different locations on Facebook's website, as follows (noting that the cookie banner is only relevant to the information provided concerning the personal data, if any, that will be processed as a result of the user having visited Facebook's website):

a. Cookie banner
b. "The Facebook Companies"
c. "The Facebook Company Products"
d. "What are the Facebook Company Products"
e. "Facebook Business Tools"

Assessment of Decision-Maker

Article 13(1)(c): the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

550. As already addressed in Part 2 of this Decision, I consider that Article 13(1)(c) requires the data controller to provide information to the data subject such that the data subject can identify what categories of personal data are processed for a particular processing operation (or set of operations) and by reference to which legal basis.

551. Considering, firstly, the extent to which the user is informed as to the categories of personal data that will be shared with the Facebook Companies, this information is only meaningfully addressed in the Facebook FAQ. While the relevant part of the Facebook FAQ states that WhatsApp "currently shares limited categories of information with the Facebook Companies", the information described appears to comprise a substantial part of the information detailed in the "Information We Collect" section of the Privacy Policy.

552. I further note that the Privacy Policy only provides a single link to the Facebook FAQ, within the "How We Work With Other Facebook Companies" section. While this is a logical place for the link, it is unclear why it has not also been included in the "Information You And We Share" section of the Privacy Policy. I note, in this regard, that numerous sections of the Privacy Policy have been (repeatedly) cross-referenced to each other via links in different sections of the Privacy Policy. Given the importance of the information contained in the Facebook FAQ, it is unclear, firstly, why it is in a stand-alone document and, secondly, why there is only a single link to it in the Privacy Policy. I further note that the link in question is embedded in "Learn more" text with the result that it does not stand out to a user wishing to access it again outside of the "How We Work With Other Facebook Companies" section of the Privacy Policy.

553. Turning, then, to the information provided concerning the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, I firstly note that there are generalised references, throughout the entire Page, as to the reasons why WhatsApp needs to share information with the Facebook Companies. By way of example, there are repeated references to keeping WhatsApp and the Facebook Companies "safe and secure". It is unclear, however, what sort of processing operations will be carried out to this end, or even what "keeping WhatsApp and the Facebook Companies safe and secure" might entail. This type of generalised information is of little benefit to the user. In terms of any less generalised information that has been provided in relation to the purpose of any sharing, this information is described and located as follows:

    a. Top of the Page and also in the Facebook FAQ:
        a. To receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and
        b. To keep WhatsApp and the Facebook Companies safe and secure

    b. Top of the Page:
        a. Provide you fast and reliable messaging and calls around the world
        b. Understand how our services and features are performing
        c. Ensure safety and security across WhatsApp and the Facebook Company Products by removing spam accounts and combatting abusive activity

d. Connect your WhatsApp experience with Facebook Company Products
e. Enable you to communicate with businesses on WhatsApp

c. "How We Work With Other Facebook Companies" section of Privacy Policy
    a. To help operate, provide, improve, understand, customize, support, and market our Services and their offerings
    b. [including] helping improve infrastructure and delivery systems
    c. Understanding how our Services or theirs are used
    d. Helping us provide a way for you to connect with businesses
    e. Securing systems
    f. Fight spam, threats, abuse or infringement activities and promote safety and security across the Facebook Company Products

d. The Facebook FAQ
    a. Services received from the Facebook Companies (and trusted third parties) include
        i. infrastructure, technologies, systems, tools, information, and expertise to help us provide and improve the WhatsApp service for our users.
            1. This enables WhatsApp to
                a. analyse and understand how our Services are being used
                    i. so as to more accurately report information about our Services and to improve our Services.
                    ii. And understand how people use WhatsApp services compared to other apps or services in the Facebook Companies, which helps us to explore potential features or product improvements
                b. explore ways to build a sustainable business
    a. To keep WhatsApp and other Facebook family services safe and secure
        ii. By helping to fight spam and abuse on our Services
        iii. Help keep our Services [safe and] secure

554. As is evident from the above, very little relevant information, in relation to the reasons why WhatsApp shares information with the Facebook Companies, is to be found in the Privacy Policy itself. The most meaningful information is to be found in the Facebook FAQ. Again, it is unclear why this document is not linked more frequently throughout the Privacy Policy, as an alternative to the meaningless and generalised information that has been included in the Privacy Policy.

555. In relation to the information provided as to the legal bases relied upon when sharing personal data with the Facebook Companies, the issues identified in Part 2 of this Decision apply here. It is impossible to identify what legal basis is relied upon by WhatsApp when it is sharing personal data with the Facebook Companies for the various purposes identified.

<u>WhatsApp's Response</u>

556. By way of the Preliminary Draft Submissions, WhatsApp firstly restated its disagreement with my view that Article 13(1)(c) requires a controller to provide information to the data subject such that the data subject can identify what categories of personal data are processed for a particular processing

operation (or set of operations) and by reference to which legal basis[217]. I acknowledge WhatsApp's position, in this regard, and have already taken account of WhatsApp's substantive submissions on this particular issue in Part 2 of this Decision.

557. WhatsApp further made the preliminary comment that it did not provide its views on compliance with Article 13(1)(c) in the context of working with the Facebook Companies in the Inquiry Submissions as the Investigator did not propose a finding under this heading[218]. While I acknowledge WhatsApp's position, in this regard, I do not consider that WhatsApp has been disadvantaged or prejudiced in any way by this in circumstances where it has already been provided with the opportunity to be heard, at the Preliminary Draft stage, on the Proposed Approach by reference to Part 2 of this Decision.

558. In relation to my comments concerning the placement of the Facebook FAQ and the fact that it is a stand-alone document, WhatsApp submitted that:

> *"The Facebook FAQ (as a stand-alone document) was first drafted on the basis of extensive consultation with the Commission. During that consultation the Commission did not take issue with the Facebook FAQ being provided as a stand-alone document. Nor has the Commission subsequently objected to maintaining the Facebook FAQ as a standalone document (on the understanding it is to be read in conjunction with the Privacy Policy which should refer to the Facebook FAQ). While WhatsApp disagrees that there is any transparency deficiency in this regard and certainly does not consider that this matter comprises an Articles [sic] 12 or 13 contravention, WhatsApp is giving further thought to the structure of this information and how best to ensure this information is prominently featured and accessible to users[219]."*

559. I have previously recorded my assessment of WhatsApp's submissions concerning its pre-GDPR engagement with the Commission's Consultation Unit as part of my assessment of WhatsApp's Submissions of General Application, at paragraphs 228 to 232, above.

560. In relation to my observations concerning the extent of information provided about the legal basis being relied upon for processing, WhatsApp contended that:

> *"As an initial point, WhatsApp would like to clarify that it does not require a distinct legal basis to share data with Facebook Companies when they are acting as its processor. With respect to sharing data with Facebook Companies on a controller-to-controller basis … WhatsApp has committed to not share any European Region WhatsApp user data for the purpose of Facebook using this data to improve their products and advertisements without prior discussion with the Commission. With respect to controller-to-controller sharing for safety and security, WhatsApp has previously explained to the Commission that: "… following the GDPR Update WhatsApp intended to commence the sharing of its EU users' data with Facebook on a controller-to-controller basis for safety and security purposes only. We made this clear to our users in the User Engagement Flow and our Privacy Policy as well as explaining to users the legal bases on which we will rely for this sharing … Whilst we plan to commence this sharing in the foreseeable future, we can confirm that WhatsApp will only do so following further*

[217] The Preliminary Draft Submissions, paragraph 14.2
[218] The Preliminary Draft Submissions, paragraph 14.3
[219] The Preliminary Draft Submissions, paragraph 14.4(B)

engagement and consultation with your Office". This notwithstanding, were WhatsApp to share European Region WhatsApp users' personal data with other Facebook Companies as controllers for this purpose, information on the legal basis that would be relied upon for this sharing is provided in the final bulleted paragraph of the general legitimate interests section of the Legal Basis Notice ("To share information with the Facebook Companies to promote safety and security"). Given the unequivocal nature of this language about reliance on legitimate interests for this sharing with Facebook Companies, WhatsApp is of the view that there is no contravention of Article 13(1)(c) GDPR[220]."

561. WhatsApp is, of course, correct that it does not require a distinct legal basis to share personal data with the Facebook Companies when they are acting as its processor. However, the Privacy Policy and related materials do not enable the reader to understand which transfers are taking place on a controller-to-processor basis and which are taking place on a controller-to-controller basis. As regards the latter, I note that WhatsApp's submissions indicate that no such transfers take place for the purpose of safety and security or for the purpose of enabling Facebook to improve its products and advertisements. It remains unclear, however, whether any personal data is being shared with the Facebook Companies on a controller-to-controller basis for any other purpose(s). Further, the inclusion of a specific legal basis to support the sharing of information "with the Facebook Companies to promote safety and security" in the Legal Basis Notice is misleading if it is the case that no such transfers are actually taking place. I note, in this regard, that there are numerous references to the sharing of personal data with the Facebook Companies in connection with "safety and security" throughout the Privacy Notice and related pages. The inclusion of a specific legal basis to support transfers matching this description misleads users by suggesting that such transfers take place on a controller-to-controller basis. This impression is also conveyed by the text used within the "How is my WhatsApp information used by the Facebook Companies?" section of the Facebook FAQ. I note, in this regard, that under the heading "(t)o keep WhatsApp and other Facebook family services safe and secure", the example provided and the absence of confirmation that the relevant data is shared with the Facebook Companies as *service providers*, in contrast to the preceding heading, strongly suggests, to the reader, that the transfers described are taking place on a controller-to-controller basis rather than on a controller-to-processor basis. I also note the express confirmation provided, in the Facebook FAQ, that WhatsApp does not share data with the Facebook Companies for the purpose of enabling Facebook to improve its products and advertisements. The absence of a similar confirmation, in relation to the sharing of data for safety and security purposes, only exacerbates the confusion caused by the misleading language used elsewhere.

562. As regards WhatsApp's having provided a legal basis for controller-to-controller processing that is not actually taking place, I note that Article 13(1)(c) requires the provision of information in relation to the "purpose of the processing for which the personal data *are intended* as well as the legal basis for the processing". The use of the words "are intended" reflects the fact that, at the point of collection, the data controller *intends* to process the data for the purposes outlined to the data subject. There may be cases where, for reasons unforeseen, the data controller is unable, or no longer wishes, to proceed with the processing once the data has been collected.

[220] The Preliminary Draft Submissions, paragraph 14.4(C)

In such a case, it would not be fair to find that a controller breached Article 13(1)(c) simply because of a change in circumstances after the initial collection of the personal data concerned. Nevertheless, I note that considerable time has elapsed since the formulation of the relevant parts of the Privacy Policy and related pages (including the Facebook FAQ) and the letter dated 8 June 2018 to the Commission, advising of WhatsApp's plan to "commence this sharing in the foreseeable future". As set out above, I consider that the inclusion of reference to a legal basis to support controller-to-controller transfers of personal data to the Facebook Companies is misleading.

563. For the sake of completeness, I do not agree with WhatsApp's assertion[221] that, "were it to commence" the sharing of personal data with the Facebook Companies for safety and security purposes, that the language used in final bulleted paragraph of the general legitimate interests section of the Legal Basis Notice satisfies the requirements of Article 13(1)(c). I have already addressed the information that must be provided, in this regard, in the corresponding section of Part 2 of this Decision. I note, in this regard, that the information provided does not identify the processing operations that will take place under this heading or the categories of personal data that will be so processed.

Article 13(1)(d): where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party

564. As set out in my assessment, in Part 2 of the Preliminary Draft, of the information provided under this heading, my preliminary view was that WhatsApp has provided clear and transparent information to users in relation to the legitimate interests being pursued. Considering this aspect of matters specifically from the point of view of the extent to which it is transparent that the legitimate interests of the Facebook Companies might form part of the legal basis for processing in respect of the sharing with them of personal data by WhatsApp, I note that the relevant sections of the Legal Basis Notice include reference to the Facebook Companies as follows:

565. Under the section addressed to people under the age of majority:

> *"The legitimate interests we rely on for this processing are:*
>
> - *To … keep our Services and all of the Facebook Company Products free of harmful or inappropriate content …"*

566. Under the section addressed to all users, including those under the age of majority:

> *"For providing marketing communications to you. The legitimate interests we rely on for this processing are:*
>
> - *To promote Facebook Company Products and issue direct marketing."*
>
> *"To share information with others including law enforcement and to respond to legal requests. See our Privacy Policy under Law and Protection for more information. The legitimate interests we rely on for this processing are:*

[221] The Preliminary Draft Submissions, paragraph 14.4(C)

> • *To prevent and address fraud, unauthorised use of the Facebook Company Products …"*
>
> *"To share information with the Facebook Companies to promote safety and security. See our Privacy Policy under "How We Work with Other Facebook Companies" for more information. The legitimate interests we rely on for this processing are:*
>
> • *To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products."*

567. I expressed the view, in the Composite Draft, that the information provided above is broadly representative of the information I would expect to see, by reference to the processing described in the Facebook FAQ.

Article 13(1)(e): the recipients or categories of recipients of the personal data, if any

568. As set out above, this information is provided mainly by way of links to "articles" on the Facebook website. However, this approach effectively forces the data subject to accept a certain level of cookie processing by Facebook if he/she wishes to access information on the identities of the "Facebook Companies". In other words, by seeking to vindicate his/her right to transparency, the data subject is subjected to processing of his/her personal data through the use of cookies. This runs counter to the nature of transparency as a freestanding right; a data subject is entitled to transparency information without any conditionality. Further, and in any event, the information available on the Facebook website is minimal so it is unclear why it has been split into three/four separate articles (which are linked to each other, in various ways) on that website. The information could easily be consolidated into a single piece of text and hosted on WhatsApp's website.

569. While the Facebook FAQ touches upon the identities of the Facebook Companies (as discussed below), I note that the user is only invited to access the Facebook FAQ document in the "How We Work With Other Facebook Companies" section of the Privacy Policy. If the user, when looking for information in relation to the recipients/categories of recipient, only reviews the "Information You And We Share" section of the Privacy Policy (which would not be an unreasonable course of action, given the title of this section), he/she is deprived of the additional information which is solely set out in the Facebook FAQ.

570. My views, in relation to the information that must be provided to a data subject, for the purpose of Article 13(1)(e), are already set out in the corresponding section of Part 2 of this Decision. Assessing this requirement specifically from the perspective of transparency in the context of the sharing of data between WhatsApp and the Facebook Companies, I note as follows:

571. Each time the term "Facebook Companies" is referenced in the Page, it contains an embedded hyperlink that, when selected, brings the user to an "article" entitled "the Facebook Companies", on Facebook's website. That "article" provides that:

> "**The Facebook Companies**
> In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below, in accordance with their respective terms of service and privacy policies. We may share information about you within our family of companies to

facilitate, support and integrate their activities and improve our services. For more information on the Facebook Companies' privacy practices and how they treat individuals' information, please visit the following links:

- Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy) and Facebook Payments International Limited (https://www.facebook.com/payments_terms/EU_privacy).
- Onavo (http://www.onavo.com/privacy_policy).
- Facebook Technologies, LLC and Facebook Technologies Ireland Limited (https://www.oculus.com/legal/privacy-policy/).
- WhatsApp Inc. and WhatsApp Ireland Limited (http://www.whatsapp.com/legal/#Privacy).
- CrowdTangle (https://www.crowdtangle.com/privacy).

…

Related Articles

The Facebook Company Products

How can I switch back to Classic Facebook?

Can I search for specific videos on the Facebook Watch TV app?

How do I get to the Facebook mobile site (m.facebook.com)?

What are the Facebook Products?"

572. Each time the "Facebook Company Products" is referenced in the Page, it contains an embedded hyperlink that, when selected, brings the user to an "article" entitled "the Facebook Company Products", on Facebook's website. That "article" provides that:

"**The Facebook Company Products**

The Facebook Company Products are, together, the Facebook Products and other products provided by the Facebook Companies that are subject to a separate, stand-alone terms of service and privacy policy, including the WhatsApp, Oculus, and CrowdTangle websites, products, or apps."

573. The term "Facebook Products", above, contains an embedded link that brings the user to another "article" on Facebook's website, entitled "Facebook Products". That "article" provides:

"**What are the Facebook Products?**

The Facebook Products include Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network, NPE Team apps and any other features, apps, technologies, software, products, or services offered by Facebook Inc. or Facebook Ireland Limited under our Data Policy. The Facebook Products also include Facebook Business Tools[2], which are tools used by website owners and publishers, app developers, business partners (including advertisers) and their customers to support business services and exchange information with Facebook, such as social plugins (like the "Like" or "Share" button) and our SDKs and APIs.

Facebook Products does not include some Facebook-offered products or services that have their own separate privacy policies and terms of service – such as Workplace, Free Basics, and Messenger Kids."

574. The term "Facebook Business Tools", above, contains a link to a further "article", as follows:

"**The Facebook Business Tools**

The Facebook Business Tools are technologies offered by Facebook Inc. and Facebook Ireland Limited that help website owners and publishers, app developers, and business partners,

> including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who use or might be interested in their products and services. These Tools include APIs and SDKs, the Facebook Pixel, Facebook social plugins, such as the Like and Share buttons, Facebook Login and Account Kit, and other Platform integrations, as well as other plugins, code, specifications, documentation, technology and services."

575. The Facebook FAQ defines the "Facebook Companies" as follows:

> **"What are the Facebook Companies?**
> WhatsApp is one of the Facebook Companies. The Facebook Companies include, among others, Facebook, Oculus, and WhatsApp and together offer the Facebook Company Products."

576. I note that the definition provided by the Facebook FAQ, above, indicates that Oculus is one of the Facebook Companies. The corresponding definition on Facebook's website, however, does not include Oculus in the "Facebook Companies" article but rather in the "Facebook Company Products" article. Oculus is included in the above text in the Facebook FAQ, alongside WhatsApp and CrowdTangle, both of which were previously defined as being "Facebook Companies", by reference to the "article" on Facebook's website.

577. Having reviewed the information provided on numerous occasions, I cannot identify, with any degree of certainty, the extent of the entities that are covered by the definition of "Facebook Companies" such as to be able to identify all of the possible recipients of user data.

578. I note, in this regard, that Exhibit 21.1 of the Form 10-K filed with the US Securities and Exchange Commission for the fiscal year ended December 31, 2018 (which is attached to the Directors' Report and Financial Statements filed with the Irish Companies Registrations Office on behalf of Facebook Ireland Limited for the financial year ended 31 December 2018) comprises a list of thirty separate corporate entities. WhatsApp is not included on that list so, presumably, the list is just a fraction of the total corporate entities making up the Facebook "family", once the subsidiaries of the listed companies are taken into account. Thirty companies alone (without any further entities which may not have been included in this list) is a very significant number of potential recipients of a user's personal data yet the user is provided with no meaningful information as to which Facebook entities will receive his/her data and for what purpose.

579. In the circumstances set out above, it is incumbent on WhatsApp to address the question of what, exactly, "Facebook Companies" means for the purposes of Article 13(1)(e). If WhatsApp wishes to address the question by reference to its current approach, the user must be able to clearly and easily identify the full extent of the entities that are covered by the term "Facebook Companies". That term, once defined for the purposes of Article 13(1)(e) should only contain the names of those "Facebook Companies" that actually receive user data from WhatsApp. Further, it should be possible for the user to access this information on WhatsApp's website and in a single, composite text (rather than a series of interlinked and overlapping "articles").

WhatsApp's Response

580. WhatsApp, by way of the Preliminary Draft Submissions, expressed its disagreement with the views I expressed under this heading, submitting firstly that "*the Facebook FAQ was first drafted on the basis of extensive consultation with the Commission and during that consultation the Commission*

did not raise concerns about the identity of the Facebook Companies or the linking to Facebook resources to provide additional information[222]*.*"

581. WhatsApp further submitted, in this regard, that:

> *"There is no requirement in the GDPR that prevents companies from referring individuals to information available from other sources and the Commission did not raise an issue with this approach previously*[223]*.*

582. My assessment of WhatsApp's submissions concerning its pre-GDPR engagement with the Commission's Consultation Unit has already been recorded as part of my assessment of WhatsApp's Submissions of General Application, at paragraphs 228 to 232, above. As regards WhatsApp's submission that there is no requirement in the GDPR that prevents companies from referring individuals to information available from other sources / provided by entities other than the controller, my view is that it is unfair to deliver the statutorily required transparency information to a data subject in a way that unnecessarily forces that data subject to accept the further collection and processing of his/her personal data by a third party. The information that WhatsApp is required to provide, in this regard, is information that is uniquely known to WhatsApp and its processors and which could easily be provided by WhatsApp. This is different to a case where, for example, a data controller might wish to include a link to the relevant part of the European Commission's website so that the data subject can learn more about the particular mechanism being relied upon to support the transfer of his/her personal data outside of the EEA. The further information available on the European Commission's website, in this regard, is not information that it uniquely known to the data controller given that it had no part to play in the implementation of the relevant transfer mechanism(s).

583. WhatsApp further submitted, under this heading, that:

> *"WhatsApp wishes to clarify that the "Facebook Companies" information on the Facebook website includes "Facebook Technologies, LLC and Facebook Technologies Ireland Limited* (https://www.oculus.com/legal/privacy-policy/) *which provides the Oculus product and is sometimes referred to as 'Oculus' (as in the Facebook FAQ) because it provides the Oculus product. The website address included after this company name clearly refers to Oculus and WhatsApp submits that it is clear that the Facebook Companies comprise of the companies listed in the "Facebook Companies" information on the Facebook website which gives more detailed information, expanding on the colloquial names of the companies listed in the Facebook FAQ*[224]*."*

584. While I accept WhatsApp's clarification of the position, I remain of the view that the identification of the "Facebook Companies", as set out in the Privacy Policy and related material, is unclear. I note, in this regard, that:

[222] The Preliminary Draft Submissions, paragraph 14.7
[223] The Preliminary Draft Submissions, paragraph 14.10
[224] The Preliminary Draft Submissions, paragraph 14.8

a. The Facebook FAQ identifies the Facebook Companies by the use of open-ended language – "include, among others, Facebook, Oculus, and WhatsApp" [emphasis added].

b. The linked "article" provides that *"(i)n addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below … ."* The corresponding list comprises eight specified companies. I note, however, this list is "*in addition to the services offered by Facebook Inc. and Facebook Ireland Ltd*." The use of the language "in addition to" is, again, open-ended, in that it suggests the existence of something in addition to the identified list of eight companies. No clarification, however, is provided as to the significance of this statement or what is meant by "the services offered", in this context.

c. The "article" further confirms that *"(w)e may share information about you within our family of companies*". It is unclear, however, what is meant by "our family of companies". It could mean the subsequent list of eight specified companies. Alternatively, it could mean the eight specified companies together with Facebook Inc. and Facebook Ireland Ltd or it might mean the eight specified companies together with Facebook Inc. and Facebook Ireland Ltd plus "the services offered".

d. The fact that Oculus is identified as being a Facebook Company Product and not a Facebook Company only exacerbates the uncertainty of the position.

585. The result of the above is the creation of doubt, in the mind of the reader, as to the extent of the entities that comprise the "Facebook Companies" for the purpose of the Facebook FAQ. Such doubt is unnecessary and could easily be eliminated by removing the open-ended language identified above and clarifying the matters which have been referred to above.

586. WhatsApp finally submitted that:

> *Without prejudice to WhatsApp's position that the manner in which the information is provided in full compliance with Article 13(1)(e) GDPR, WhatsApp will make this information available on the WhatsApp website when making the suite of changes to its Privacy Policy and user facing information[225]."*

587. I acknowledge WhatsApp's commitment to making the relevant information available on its own website. My assessment of WhatsApp's Submissions of General Application, in Part 2 of this Decision, includes an assessment of any submissions made concerning WhatsApp's willingness to incorporate changes, on a voluntary basis, to its privacy material.

Finding: Assessment of compliance with the requirements of Articles 13(1)(c), 13(1)(d) and 13(1)(e)

588. As set out above, the information that has been provided, regarding WhatsApp's relationship with the Facebook Companies and the data sharing that occurs in the context of that relationship, is spread out across a wide range of texts and a significant amount of the information provided is so high level as to be meaningless. While the Facebook FAQ is a comprehensive and informative document, it is

[225] The Preliminary Draft Submissions, paragraph 14.10

only linked to the Privacy Policy in one place (via the "Learn More" link at the end of the end of the "How We Work With Other Facebook Companies" section). While WhatsApp has referenced "numerous other FAQs" available on its website, in this regard, it is unfair to expect the user to search WhatsApp's website, after having failed to find sufficient information in the Privacy Policy itself.

589. In relation to the inclusion of text concerning, or suggesting, the existence of controller-to-controller sharing of personal data with the Facebook Companies for safety and security purposes, this text is misleading by reference to the confirmation provided in the Preliminary Draft Submissions that no such processing has ever taken place. If the commencement of such processing is not imminent, such text should be removed from the Legal Basis Notice and Facebook FAQ so as to avoid misleading the user. If, however, WhatsApp intends to imminently proceed with the commencement of such processing, my view is that the Facebook FAQ and Legal Basis Notice do not sufficiently inform the data subject as to the legal basis that will be relied upon for any such processing. My views, in this regard, are already set out as part of my assessment of the extent to which WhatsApp provides the information prescribed by Article 13(1)(c). Those views apply equally here.

590. Further, it is unsatisfactory that the user has to access information as to the identity of the Facebook Companies on Facebook's website and for the information to be broken up over three or four different "articles" that each link back to one another in a circular fashion. There is no reason why this information could not be hosted, in a concise piece of text, on WhatsApp's website. As set out above, the information currently being provided is unnecessarily confusing and ill-defined. As set out in Part 2 of this Decision, it is a matter for a data controller to determine how best to provide the required information to data subjects. In this case, there is an over-supply of very high level, generalised information at the sacrifice of a more concise and meaningful delivery of the essential information. Where links and layering are used, they should be used in a considered way that ensures the concise and meaningful delivery of the required information. In this case, however, it is a matter of luck, rather than logic, as to whether or not the user will access the information provided in the Facebook FAQ. If the user has engaged with the other, less meaningful (and, in one place, contradictory) information en route, this may undermine the user's ability to *receive* the information set out in the Facebook FAQ.

591. **Accordingly, for the reasons set out in the composite analysis, above, I find that WhatsApp has failed to comply with its transparency obligations pursuant to Articles 13(1)(c), 13(1)(e) and 12(1) in relation to how WhatsApp works with the Facebook Companies. I further direct that, unless WhatsApp has a concrete plan in place, that includes a definitive and imminent commencement date, to commence the sharing of personal data on a controller-to-controller basis with the Facebook Companies for safety and security purposes, the misleading elements of the Legal Basis Notice and Facebook FAQ should be deleted to reflect the true position.**

592. For the avoidance of doubt, the Composite Draft proposed a finding that WhatsApp had broadly complied with its obligations under Article 13(1)(d) for the purpose of this Part 3. Given that the rationale was premised partly upon the original assessment of the extent to which WhatsApp had achieved compliance with Article 13(1)(d), as recorded in Part 2 of the Preliminary Draft, I must now amend my proposed finding, under this heading, in order to take account of the counter view of the Board (as recorded in the Article 65 Decision[226]), on the extent to which WhatsApp has achieved

[226] The Article 65 Decision, paragraph 66

compliance with its obligations under Article 13(1)(d). Accordingly, on the basis of paragraphs 414 to 415, above, and adopting both the binding determination and associated rationale of the Board[227] as required by Article 65(6), this Decision **finds that WhatsApp has also failed to comply with its obligations pursuant to Article 13(1)(d) in relation to how WhatsApp works with the Facebook Companies**.

Part 4: Article 5(1)(a) - Extent of Compliance with the Principle of Transparency

Introduction

593. As noted in paragraph 1 of this Decision, the scope of the underlying inquiry carried out by the Commission concerned the extent to which WhatsApp has complied with the obligations arising pursuant to Articles 12, 13 and 14 of the GDPR. That being the case, the Composite Draft did not contain any assessment or proposed finding in relation to the extent to which WhatsApp might be said to have complied with the overarching general principle of transparency set out in Article 5(1)(a) of the GDPR. This notwithstanding, objections were raised by the Hungarian and Italian SAs concerning the absence of a proposed finding under this heading. Further to an initial assessment, the Board determined that only the objection raised by the Italian SA was "relevant and reasoned" for the purpose of Article 4(24).

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

594. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, this matter was included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objection raised by the Italian SA, the Board determined[228] as follows:

> *184. "The IT SA argues that, given that transparency has been identified by the IE SA as the core of the Inquiry, and the Draft Decision contains findings of infringements of articles 12 to 14 GDPR, the Draft Decision should also contain a finding of non-compliance with article 5(1)(a) GDPR. The IT SA argues that "Article 5(1)a. is a provision of a general nature setting forth one of the seven key principles underlying the whole framework of the Regulation." The IT SA also observes that the Draft Decision refers "cursorily to Article 5(1)a. in various passages [...], however it does not ultimately draw the conclusion that there was an infringement of that provision as well". Finally, the IT SA considers that the finding of an infringement of such provision would not undermine WhatsApp IE's right to be heard, given that "this is a provision of a general, overarching nature compared to Articles 12 to 14 GDPR, so that WhatsApp's defence regarding those Articles may be automatically relayed back to the general principle as well" [229].*
>
> *185. In the Composite Response, the IE SA acknowledges that "[h]aving considered this objection against the backdrop of the existing scope, facts identified and provisional findings previously notified to WhatsApp concerning various infringements of Articles 12, 13 and 14, IE SA considers, on a preliminary basis, that a finding that WhatsApp has*

[227] The Article 65 Decision, paragraphs 42 to 66 (inclusive)
[228] The Article 65 Decision, paragraphs 183 to 201 (inclusive)
[229] Footnote from the Article 65 Decision: IT SA Objection 1.c., page 5.

infringed Article 5(1)(a) insofar as it concerns transparency potentially may arise from the various findings of infringement of the more specific transparency obligations which are set out in the Composite Draft" [230].

186. In its submissions, WhatsApp IE outlined two different possible approaches. First, if the objections are premised on the assumption that a finding of non-compliance with Articles 12 to 14 GDPR must equate automatically to non-compliance with Article 5(1)(a) GDPR, they are insufficiently relevant and reasoned and from a procedural perspective the controller cannot be punished twice for the same conduct [231]*. In this regard, WhatsApp IE agrees with the statement by the FR SA (which "fails to see on which facts, not already covered by the breach to article 12, the breach to article 5(1)(a) would be based" and "wonders if [the addition of fines in respect of such additional infringements] would be compatible with the principle according to which the same facts should be punished only one time"* [232]*).*

187. Second, WhatsApp IE argues that according to the second approach, compliance with Article 5(1)(a) GDPR addresses something different to the provision of prescribed information in an appropriate manner, and would be a "more expansive principle, holistically encapsulating transparency, fairness and lawfulness," and arguably concerned with the justifiability of a processing operation rather than with whether prescribed items of information have been provided [233]*. Therefore, it would be possible for a processing operation to comply with Articles 12-14 GDPR and fall short of Article 5(1)(a) GDPR or vice versa* [234]*. More specifically, "a* ***technical contravention of Articles 12 to 14 GDPR would not necessarily give rise to a "transparency" failure under Article 5(1)(a) GDPR, if the controller has nonetheless made data subjects aware of the processing in question"*** [235]***.*** *WhatsApp IE submits that it complied with the obligations under Article 5(1)(a) GDPR in full, as it is a controller that has committed considerable resources to engaging with its users "and that publishes comprehensive information on its processing: therefore, even if it was found that information provided to data subjects was insufficiently granular or could have been provided in a different manner (such that there has been a technical contravention of Articles 12 to 14 GDPR), it would not necessarily follow that such a controller could be considered to be acting in an unfair or non-transparent manner which infringes Article 5(1)(a) GDPR"* [236]*. Also, if Article 5(1)(a) GDPR imposes a separate and distinct obligation, WhatsApp IE states that it meets these obligations, and this did not fall within the scope of the Inquiry, which means that WhatsApp IE needs to speculate as to what the case against it might be and is not in a position to exercise its full right to be heard* [237]*. According to WhatsApp IE, it would be procedurally unfair to incorporate a finding on this issue at this stage, also because it should have a proper opportunity to reply*

[230] Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 18(a)(i), as referred to in paragraph 20 (emphasis added).
[231] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraphs 12.1 and 13.2(A). See also 35.22-35.24 (concerning the interpretation of Article 83(3) GDPR but referring to the principle of *ne bis in idem* as enshrined in Article 50 of the Charter).
[232] Footnote from the Article 65 Decision: FR SA Response, page 2.
[233] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.2.
[234] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.3.
[235] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.3.
[236] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.3.
[237] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.1.

to fully reasoned arguments as to why there has been an alleged distinct infringement of Article 5(1)(a) GDPR [238].

188. The EDPB notes that the concept of transparency is not defined as such in the GDPR. However, Recital 39 GDPR provides some elements as to its meaning and effect in the context of processing personal data. As stated in the Transparency Guidelines, this concept in the GDPR "is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles" [239]. The key provisions concretising the specific practical requirements of transparency are in Chapter III GDPR. However, there are other provisions that also realise the transparency principle, for example, Article 35 (data protection impact assessment) and Article 25 GDPR (data protection by design and by default), to ensure that data subjects are aware of the risks, rules and safeguards in relation to the processing, as stated in Recital 39 GDPR [240].

189. The EDPB also notes that transparency is an expression of the principle of fairness in relation to the processing of personal data and is also intrinsically linked to the principle of accountability under the GDPR [241]. In fact, as noted in the Transparency Guidelines, a central consideration of the principles of transparency and fairness is that "the data subject should be able to determine in advance what the scope and consequences of the processing entails" and should not be taken by surprise about the ways in which their personal data has been used [242].

190. Thus, it is apparent that, under the GDPR, transparency is envisaged as an overarching concept that governs several provisions and specific obligations. As stated in the Transparency Guidelines, "[t]ransparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights" [243].

*191. This being said, it is important to differentiate between **obligations stemming from the principle of transparency and the principle itself**. The text of the GDPR makes this distinction, by enshrining transparency as one of the core principles under Article 5(1)(a) GDPR on the one hand, and assigning specific and concrete obligations linked to this principle, on the other one. The concretisation of a broad principle in specific rights and obligations is not a novelty in EU law. For example, with regard to the principle of effective judicial protection, that CJEU has stated that it is reaffirmed in the right to an effective remedy and to a fair hearing, enshrined in Article 47 of the Charter [244]. Nonetheless, that does not imply that principles as such cannot be infringed. In fact, under the GDPR the*

[238] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 13.2(B). WhatsApp further argues that it is inappropriate for it not to have the case for infringement put to it in line with the other issues in scope of the inquiry and instead be required to make submissions in the abstract in response to insufficiently particularised reasoning as to the meaning and application of Article 5(1)(a) GDPR where WhatsApp does not have adequate notice of the nature of the case being made against it.

[239] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4.

[240] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 42.

[241] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 2.

[242] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 10.

[243] Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 1.

[244] Footnote from the Article 65 Decision: Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy, (Case C-73/16, judgment delivered 27 September 2017) ECLI:EU:C:2017:725, paragraph 59.

infringement of the basic principles for processing is subject to the highest fines of up to 20.000.000€ or 4% of the annual turnover, as per Article 83(5)(a) GDPR.

192. On the basis of the above considerations, the EDPB underlines that the principle of transparency is not circumscribed by the obligations under Articles 12-14 GDPR, although the latter are a concretisation of the former. Indeed, the principle of transparency is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive. In addition, as stated above, Article 83(5) GDPR includes the possibility to find an infringement of transparency obligations independently from the infringement of transparency principle. Thus, the GDPR distinguishes the broader dimension of the principle from the more specific obligations. In other words, the transparency obligations do not define the full scope of the transparency principle.

193. That being said, the EDPB is of the view that an infringement of the transparency obligations under Articles 12-14 GDPR can, depending on the circumstances of the case, amount to an infringement of the transparency principle.

194. In this particular case, the question that the EDPB is confronted with is whether the infringements of specific transparency obligations by WhatsApp IE amount to an infringement of the overarching principle of transparency under Article 5(1)(a) GDPR.

195. In the draft decision, the IE SA considers that WhatsApp IE has not complied with the following obligations under the GDPR with regard to the information provided to users of the service: obligations pursuant to Articles 13(1)(c) and 12(1) [245]; 13(1)(e) and 12(1) [246]; 13(1)(f) and 12(1) [247]; 13(2)(a) [248]; and 13(2)(c) and 12(1) GDPR [249]. With regard to non-users, the IE SA considers that WhatsApp IE has infringed its obligations under Article 14 GDPR, albeit noting that the personal data undergoing processing is very limited [250]. Finally, with regard to the transparency obligations in the context of sharing user data between WhatsApp IE and Facebook Companies, the IE SA considers that Articles 13(1)(c), 13(1)(e) and 12(1) have been infringed [251].

196. On the contrary, the IE SA did not find any infringement with regard to Articles 13(1)(a)-(b), 13(1)(d) and 13(2)(d) GDPR. With regard to Article 13(1)(d) GDPR, the EDPB reached the conclusion described in paragraph ***Error! Reference source not found.*** *above.*

197. The EDPB also notes that, in its Composite Response, the IE SA recalls that the Draft Decision contains a finding whereby "the information provided by WhatsApp , in relation to its data processing operations and the legal basis/bases being relied upon to support any such processing, is so inadequate that it is not possible to identify: i) the specific processing operations taking place; (ii) the purpose of those processing operations; or (iii) the legal basis being relied upon to ground those processing operations" [252]. Indeed, the Draft Decision recalls that "it is impossible [for the IE SA] to understand which legal basis might be relied on for any particular act of processing" [253], and that "it is self-evident

[245] Footnote from the Article 65 Decision: Draft Decision, paragraph 385.
[246] Footnote from the Article 65 Decision: Draft Decision, paragraph 417.
[247] Footnote from the Article 65 Decision: Draft Decision, paragraph 440.
[248] Footnote from the Article 65 Decision: Draft Decision, paragraph 458.
[249] Footnote from the Article 65 Decision: Draft Decision, paragraph 479.
[250] Footnote from the Article 65 Decision: Draft Decision, paragraphs 167-168.
[251] Footnote from the Article 65 Decision: Draft Decision, paragraph 572.
[252] Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 16.
[253] Draft Decision, paragraph 598.

[...] that there is a significant information deficit" which is exacerbated by the inaccessibility of the information[254]. This inaccessibility is also reflected in the Draft decision, with the IE SA stating that the assessment of the material "was a needlessly frustrating exercise that required the extensive and repeated search of the Privacy Policy and related material to try and piece together the full extent of the information that had been provided" [255]. The IE SA considers that the deficiencies identified are such that the users "cannot make informed decisions in relation to whether or not they wish to continue using the service" [256] and that they may also be "deprived of the information they need to exercise their data subject rights" [257]. In fact, the IE SA's assessment is that WhatsApp IE failed to provide 41% of the information required by Article 13 GDPR [258]. With regard to non-users, the IE SA considers that there has been a "total failure" to provide them with the required information. This information is "vitally important so as to enable the non-user to make an informed choice, in the event that he/she might consider joining the Service" [259].

*198. In short, the IE SA considers that the infringements found in the Draft Decision "reflect a significant level of non-compliance" which impact on **all** of the processing carried out by WhatsApp IE [260].*

*199. Taking all the above into consideration, the EDPB is of the view that, in this particular case, **there has been an infringement of the transparency principle under Article 5(1)(a) GDPR, in light of the gravity and the overarching nature and impact of the infringements**, which have a significant negative impact on all of the processing carried out by WhatsApp IE.*

200. Furthermore, the EDPB considers that WhatsApp IE has been provided the right to be heard on this issue, contrary to its claims, since it had the opportunity to express its point of view on the objections raised by the CSA on this matter [261].

201. Therefore, the EDPB decides that the IE SA is required to amend its Draft Decision in order to include a finding of an infringement of the transparency principle enshrined in Article 5(1)(a) GDPR."

595. **On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision <u>finds that WhatsApp has failed to comply with its obligations pursuant to Article 5(1)(a) of the GDPR</u>.**

Part 5: Exercise of Corrective Powers

[254] Draft Decision, paragraph 599.
[255] Draft Decision, paragraph 598.
[256] Draft Decision, paragraph 626.
[257] Draft Decision, paragraph 630.
[258] See, e.g. Draft Decision, paragraph 746.e.
[259] Draft Decision, paragraph 155.
[260] Draft Decision, paragraph 769 (emphasis added).
[261] See, in particular, sections 10-14 of WhatsApp Article 65 Submissions.

Introduction

596. Having recorded my views and findings as to whether or not an infringement of the GDPR has occurred/is occurring, I must now consider whether or not the findings of infringement merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

Approach to submissions furnished by WhatsApp in response to the Supplemental Draft

597. WhatsApp has furnished extensive submissions in response to the Supplemental Draft. Broadly speaking, those submissions can be divided into two categories:

    a. submissions directed to a specific aspect of the manner in which I assessed or proposed to apply, in the Supplemental Draft, the provisions of Article 58(2) and/or Article 83; and

    b. submissions concerning recurring themes, such that they are directed to an approach that I took, on a preliminary basis, in the Supplemental Draft generally or, otherwise, that have been directed to a number of the individual aspects of my preliminary assessment and/or proposed application of Articles 58(2) and/or Article 83 ("**Submissions on Recurring Themes**").

598. In relation to the first category of submissions, I have recorded how I have taken account of the particular submissions made in the corresponding assessment of this Part 5. In relation to the Submissions on Recurring Themes, however, I have, as a procedural economy and with a view to avoiding unnecessary duplication, recorded my views on the particular subject-matter arising in this section of the Decision only. Thus, where, as part of its response to my assessment of any individual aspect of Article 58(2) and/or Article 83, WhatsApp has indicated reliance on any matter covered by the Submissions on Recurring Themes, the views set out below should be understood as being my views on the relevant subject-matter.

WhatsApp's Submissions on Recurring Themes

599. The Submissions on Recurring Themes can be grouped into six categories, as follows:

    a. Submissions that:
        i. assert that the provisional views expressed by the Commission represent new and subjective interpretations of the transparency provisions; and/or
        ii. assert that the approach proposed by the Commission represents an alternative or higher standard of compliance, of which WhatsApp has not had prior notice; and/or
        iii. concern WhatsApp's reliance on the Transparency Guidelines; and/or
        iv. concern the flexibility afforded to data controllers, in terms of how they might achieve compliance with the transparency provisions.

    b. Submissions concerning:
        i. the nuanced nature of a transparency assessment; and/or
        ii. the significance of the differing views as between the Investigator and Decision-Maker.

    c. Submissions concerning:

i. the binary approach of the Commission, as regards the preliminary assessment of the extent of information provided to users and non-users pursuant to Articles 13 and 14; and/or
ii. the characterisation of the proposed infringements.

d. Submissions in relation to:
i. WhatsApp's careful and good faith efforts to achieve compliance with the transparency provisions; and/or
ii. WhatsApp's view that its approach is aligned with the approach adopted by many industry peers; and/or
iii. WhatsApp's pre-GDPR engagement with the Commission.

e. Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related materials, on a voluntary basis;

f. Submissions that:
i. the Commission has not demonstrated how WhatsApp's approach to transparency has in fact had any negative impact on data subject rights; and/or
ii. the Commission's concerns that the alleged infringements have impacted on data subjects' rights is theoretical and not supported as a matter of fact; and/or
iii. the Commission's analysis of the damage allegedly suffered by data subjects is based on assertions rather than evidence; and/or
iv. no evidence has been provided to indicate that WhatsApp's approach to providing transparency has undermined the effective exercise of the data subject rights.

600. For the purpose of this Decision, I have considered the above submissions as follows:

*Submissions that the preliminary views expressed by the Commission represent new and subjective interpretations of the transparency provisions and/or that the approach proposed by the Commission represents an alternative or higher standard of compliance of which WhatsApp has not had any prior notice and/or concerning the flexibility afforded to data controllers, in terms of how they might achieve compliance with the transparency provisions ("the **New and Subjective Views Submissions**")*

601. WhatsApp has submitted, in this regard[262], that:

> *"Most of the Commission's proposed findings of infringement turn on new and subjective interpretations of Articles 12 and 13 GDPR. These interpretations go beyond the letter of – and any guidance published to date in relation to – Articles 12 and 13 GDPR. As evidence of this, WhatsApp is not aware of any controller that could be considered to comply with the Commission's expectations in this regard. WhatsApp submits that it cannot be the case that unprecedented fines should be imposed on a controller in respect of findings of infringement arising from the application of standards which it was not aware of in advance, in the first case where such standards are articulated[263]."*

[262] The submissions falling under this particular heading are set out in paragraph 1.3, paragraph 1.5, paragraph 3.4(B)(2), paragraph 5.13, paragraph 5.14, paragraph 5.19, paragraph 5.20, paragraph 6.4(C) and (D) and paragraph 10.2 of the Supplemental Draft Submissions
[263] The Supplemental Draft Submissions, paragraph 1.3, paragraph 3.4(B)(2)

602. WhatsApp further submits that:

> *"The Commission's position in the Preliminary Draft in fact goes beyond simply providing the information listed in Article 13 GDPR: … For example, complying with the Commission's "Proposed Approach" requires more than simply providing information listed in Article 13(1)(c) GDPR. Ultimately, there is no clear consensus on what amounts to an appropriate approach to transparency … In these circumstances, WhatsApp submits that it cannot be held to have acted negligently … The Commission's standards go beyond that required by Article 13[264]."*

603. WhatsApp has also submitted, in this regard, that it:

> *"… should not be penalised for the duration of the alleged infringements in circumstances where it proactively sought to make changes as soon as it was in a position to understand the Commission's views[265]."*

604. In relation to the flexibility afforded to the data controller, WhatsApp has submitted that:

> "*Articles 12 to 14 GDPR collectively, by their very nature, also afford latitude to controllers in relation to how they achieve compliance, as underlined by the [Transparency Guidelines] which explicitly recognises that there are "nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area". This is an important point to bear in mind where the proposed findings of infringement … arise from the Commission and WhatsApp adopting different good faith interpretations of how to comply in practice with the broad transparency obligations set out in the GDPR – an issue which is not black and white, but dependent on subjective judgment and evaluation of what is appropriate in specific circumstances. … the Commission … should also adopt an approach which takes account of the flexibility afforded to controllers in discharging their transparency obligations as envisaged by the GDPR and by the EDPB[266]."*

605. I note that I have already assessed the substance of this particular category of submissions in the context of my assessment of WhatsApp's Submissions of General Application set out at paragraph 218 to 224 in Part 2 of this Decision (by reference to the category of "Submissions concerning Legal Certainty"). The views so expressed apply equally here. By way of summary of my position: I do not agree that the views expressed in Parts 2 or 3 of this Decision represent a new or subjective approach and neither do I accept that they represent an alternative or higher standard of compliance. I am, in fact, satisfied that my views accord with the views expressed by the Article 29 Working Party in the Transparency Guidelines, as endorsed and adopted by the EDPB on 25 May 2018.

606. I note, in any event, that there are clear inconsistencies, as between the contents of the Transparency Guidelines and the approach taken by WhatsApp. By way of example, the Transparency Guidelines provide that:

---

[264] The Supplemental Draft Submissions, paragraph 6.4(D)
[265] The Supplemental Draft Submissions, paragraph 5.20
[266] The Supplemental Draft Submissions, paragraph 1.5

"The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear[267]."

607. They further provide that:

"Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided[268]."

608. Had WhatsApp followed these directions (which, I note, were supplemented and further explained by way of examples in the corresponding sections of the Transparency Guidelines), it would have avoided the confusion that has resulted from the manner in which it formulated its Legal Basis Notice. As identified in Parts 2 and 3 of this Decision, this is a significant cause for concern, given the complete lack of clarity as to the legal basis being relied on for any of the general processing initiatives identified. Further, WhatsApp would have avoided the ambiguity that results from the use of language qualifiers, as noted in Parts 2 and 3 of this Decision.

609. In the circumstances, I am unable to attribute weight, as a mitigating factor for the purpose of my assessment as to the application of corrective powers within this Part 5, to the matters raised under this particular heading of submission. As set out above, I disagree that my views represent a different standard of compliance than that already required by the Transparency Guidelines. If, however, I am (wholly or partially) incorrect in this assessment (and, for the record, I do not consider that I am), I note that, despite its submission[269] that it relied on the Transparency Guidelines when preparing the Privacy Policy and related material, there are clear inconsistencies between the contents of WhatsApp's user-facing information and the Transparency Guidelines.

*Submissions concerning the nuanced nature of a transparency assessment and/or the significance of the differing views, as between the Investigator and Decision-Maker (the "**Nuanced Nature of Assessment Submissions**")*

610. WhatsApp has submitted, in this regard, that:

"The subjective and nuanced nature of assessing transparency – which is what renders the Commission's binary approach inappropriate – is also underlined by the fact that differing views have been reached even within the Commission throughout this Inquiry. … If transparency was simple and straightforward as the Commission asserts in the Supplemental Draft then … these material differences of opinion even within the Commission would not have arisen[270]."

611. For the reasons explained above, I do not agree that the assessment of transparency is a "subjective and nuanced" matter. While WhatsApp has sought to rely on the statement, in the Transparency Guidelines, that there are "*nuances and many variables which may arise in the context of the*

[267] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), pages 8/9
[268] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 9
[269] The Preliminary Draft Submissions, paragraph 2.1
[270] The Supplemental Draft Submissions, paragraph 5.2 (see also paragraphs 5.3 and 5.13)

transparency obligations of a specific sector, industry or regulated area[271]", this statement is simply a reflection of the fact that there is no "one size fits all" approach to transparency. In fact, I consider that WhatsApp has taken this statement from the Transparency Guidelines out of context, as its objective is to explain how the Transparency Guidelines are generally applicable to *all controllers*, irrespective of sector, industry or regulated area and to explain why the guidelines did not specifically focus on, or consider, the particular application of the transparency principle in any particular sector, industry or regulated area. Articles 13 and 14 require the provision of specified information so as to enable the data subject to understand how and why his/her personal data will be processed in the context of the particular processing that will be carried out by the data controller concerned. The Transparency Guidelines aim to provide support to data controllers, in terms of explaining how they might individually tailor the transparency requirements to the unique circumstances of their processing operations. This is clear from the introduction to the Transparency Guidelines:

> *"… these guidelines are intended to enable controllers to understand, at a high level, [the Working Party's] interpretation of what the transparency obligations entail in practice and to indicate the approach which [the Working Party] considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures*[272]*".*

612. While there will undoubtedly be "nuances" and variables, in terms of the information required to be provided, from data controller to data controller, these "nuances" and variables are the consequence of the difference in processing operations being carried out, from data controller to data controller. This does not mean, however, that there are "nuances" and variables in relation to the manner of assessment of the information provided, as considered further below, in the context of the Binary Approach Submissions. The Transparency Guidelines make it absolutely clear that the principles enunciated must be applied across the board, while acknowledging that particular measures (which still adhere to those principles) may be necessitated, depending on context.

613. In relation to WhatsApp's submissions concerning the significance of any "material difference of opinion" as between the Investigator and myself, I firstly note that there are only three such material differences, as follows:

    a. The Investigator was of the view that the information provided by WhatsApp did not satisfy the requirements of Article 13(1)(a). She formed this view on the basis of the inconsistencies, as between the Privacy Policy and the Terms of Service, in the language used to identify what is meant by the term "we". I reached a different conclusion, by reference to WhatsApp's submission that the Privacy Policy is the "primary information and transparency document in respect of WhatsApp's data processing[273]". I concluded, above, that the Privacy Policy clearly identified WhatsApp as being the relevant data controller. As regards the significance of this difference of opinion, as between the Investigator and myself, there are two observations that I would make, in this regard:

[271] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), paragraph 1
[272] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), paragraph 1
[273] The Inquiry Submissions, paragraphs 6.1 and 6.2

i. Firstly, WhatsApp created the circumstances in which it was possible for there to be a difference of opinion by using "we" in the Privacy Policy to denote WhatsApp Ireland Limited and the same term – "we" – in the Terms of Service to collectively refer to WhatsApp Ireland Limited and WhatsApp, Inc. This could have been avoided by a more careful approach to the defined term.

ii. Secondly, our difference of opinion reflected a difference in our respective approaches to the inquiry, rather than a difference in our approach to the assessment of Article 13(1)(a) itself. As already reflected in the corresponding assessment in Part 2, I focused my assessment, for the purpose of Article 13(1)(a), on the Privacy Policy because this was identified, by WhatsApp, as being the relevant primary source of the prescribed information under assessment.

b. The second difference of opinion arose in relation to our respective assessments of Article 13(2)(c). This provision requires the data controller to inform the data subject about "the existence" of the right to withdraw consent. The Investigator was satisfied that WhatsApp had done so. I reached a different finding, on the basis that, firstly, WhatsApp failed to include the full extent of the text required by Article 13(2)(c). More importantly, however, I noted that the existence of this right was not referenced in the "How You Exercise Your Rights" section of the Privacy Policy. This section, as the title suggests, is the primary source of information on the data subject rights, in the context of WhatsApp's Privacy Policy. In the circumstances, I expressed the preliminary view, which I have maintained in this Decision, that this section is where the data subject is most likely to visit, if he/she wishes to learn about his/her rights. Accordingly, it is incumbent on WhatsApp to include reference to the right to withdraw consent in this particular location. Otherwise, it is a matter of chance as to whether or not the data subject receives the information prescribed by Article 13(2)(c). Again, I note this difference in opinion, as between the Investigator and myself, is more reflective of a difference in our respective approaches to the inquiry rather than a difference in approach to the assessment of Article 13(2)(c) itself. The Investigator, in this regard, adopted a thematic / functional approach to assessment. I adopted a more formulaic approach whereby I assessed, in a holistic manner, the information that had been provided pursuant to each of the individual categories of information prescribed by Article 13.

c. The third difference of opinion arose in relation to our respective assessments of Article 13(1)(d). That difference of opinion, however, is limited to our views concerning the question of whether or not the information provided indicated the "owner" of the legitimate interests being pursued. In all other respects, the Investigator and I were aligned in our views. As already observed, the Investigator and I adopted different approaches to the inquiry. The consequence of this is apparent within our respective conclusions on the extent to which WhatsApp has complied with its obligations pursuant to Article 13(1)(d). The Investigator's Proposed Finding 9 reflected an infringement of "*a cumulative requirement, which results in Articles 13(1)(c) and 13(1)(d) operating together …*". My proposed finding, however, was based purely on an assessment of Article 13(1)(d), although I clearly noted, as part of my assessment[274], the impact of the shortcomings previously identified, pursuant to my Article 13(1)(c) assessment, on the quality of information provided in pursuance of Article 13(1)(d).

[274] The Preliminary Draft, paragraph 265

This remains the case, notwithstanding the determination of the Board on the objections raised by the German (Federal), Polish and Italian SAs concerning the Article 13(1)(d) assessment (as addressed in Part 2, above).

614. I note that the only other differences, between the Investigator and myself, are the result of a divergence in approach to the inquiry itself, rather than a divergence in approach to the transparency assessment. Unlike the Investigator, I did not propose individual findings on the manner in which the material is presented, for example, in relation to the use of layering or the suitability of language used where the recipient is likely to be under the age of majority. This is because I adopted a holistic approach to the transparency assessment whereby the only question for determination was whether or not the prescribed information had been provided. In having taken this approach, I assessed the quality of information provided, by reference to any particular category, at the same time as assessing the manner in which that information had been provided. I note that, even with this adjusted approach to the inquiry, my views, in relation to the transparency deficiencies arising from the manner in which the information had been presented, are entirely consistent with those of the Investigator.

615. In the circumstances set out above, I do not accept that the limited differences in opinion, as between the Investigator and myself, are suggestive of anything other than a thorough and robust inquiry process in which WhatsApp has been afforded the benefit of a second and independent review of matters by the Decision-Maker. Accordingly, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under this heading.

*Submissions concerning the binary approach of the Commission, as regards the preliminary assessment of the extent of information provided to users and non-users pursuant to Articles 13 and 14 and/or the characterisation of the proposed infringements (the "**Binary Approach Submissions**")*

616. WhatsApp has submitted[275], in this regard, that:

> *"The Commission's binary approach of finding either full compliance or complete non-compliance with each provision – resulting in the creation of a "55%" compliance figure – is based on its subjective views, not on any established precedent or published guidance, and does not take adequate account of the fact that the relevant information has, WhatsApp submits, been provided for each specific Article 13 category. Adopting the Commission's methodology as set out in the Supplemental Draft, WhatsApp would achieve the same 55% compliance level if it had provided no information at all in relation to the five categories concerned. … an examination of WhatsApp's transparency information against the requirements of Article 13 GDPR in fact shows that the essence of the GDPR requirements is adhered to. While it may be that, in its view, such information does not reach the new standards for compliance set by the Commission … it is certainly not the case that WhatsApp has provided no relevant information whatsoever[276]."*

617. WhatsApp further submits that:

[275] The submissions falling under this particular heading are set out in paragraph 5.1, paragraph 5.3, paragraph 5.13, paragraph 5.15, paragraph 5.30, paragraph 5.31, paragraph 8.2, paragraph 16.6(A), paragraph 5.4 and paragraph 5.6 of the Supplemental Draft Submissions

[276] The Supplemental Draft Submissions, paragraphs 5.1 and 5.13

"… the flaws in the binary approach … are particularly evident in circumstances where it is clear that: … (ii) … the Commission has not identified any provision of Article 13 GDPR where WhatsApp has failed to provide at least some information. The Commission has instead reached a more nuanced finding: namely that, in its opinion, WhatsApp should have provided more granular information in addition to what it currently provides, included more examples, or presented the information in a different manner. These alleged infringements do not support the Commission's approach of applying the Article 83(2) Factors as if WhatsApp had done nothing at all in relation to compliance with the relevant provisions. …[277]"

618. Is important to recall that the assessment with which we are, here, concerned is the obligation to provide information. I have not, by way of my assessment, sought to apply any particular standard of compliance: my view is that there could only ever be one applicable standard or test and that is the simple question of whether or not the required information has been provided. As reflected upon in Parts 2 and 3 of this Decision, effective communication simply requires the data controller to set out, for the data subject, the information described in Articles 13 and/or 14 and to do so in a way that makes it possible for the data subject to receive and understand that information. My focus, throughout my assessment, has been on the simple question of whether the Privacy Policy and related materials enabled me to receive the information that a data subject is entitled to receive, pursuant to Articles 13 and 14.

619. WhatsApp has sought to characterise my findings being "nuanced", such that they are findings that WhatsApp ought to have provided "more granular information" or more examples or, otherwise, that WhatsApp ought to have presented the information "in a different manner". I strongly disagree with this characterisation. To ensure that my assessments, views and proposed findings are understood in their proper context, and to ensure that there is no doubt as to the seriousness of the issues identified, I have summarised, below, the difficulties that I encountered when carrying out my assessment of the Privacy Policy and related materials. It is important to recall, in this regard, that, as a member of the Commission, I am experienced in data protection matters and so the review of transparency material ought to be a relatively simple exercise in circumstances where I know what I am looking for and can identify it quickly, when it is presented. A data subject may not have the same level of understanding of data protection matters; indeed, there is likely to be significant variation in this state of knowledge, as between one data subject and the next. The transparency obligation has particular significance for those data subjects who might not have a developed state of awareness of data protection matters. Thus, while, during the course of my assessment, I actively located and reviewed, in a comprehensive manner, all of the information that had been provided by WhatsApp in relation to each individual category of prescribed information, it is unlikely that an individual data subject would adopt such a complete approach. This is why it is so important that a data controller not only provides the prescribed information but provides it in such a way that it is easy for the data subject to receive it. If either of these elements is missing, it creates a situation whereby it is a matter of chance as to whether or not the data subject will achieve the state of knowledge that Articles 12 – 14 of the GDPR intend for him/her to have.

620. My experience of interacting with, and navigating, the Privacy Policy and related materials was one whereby:

[277] The Supplemental Draft Submissions, paragraph 5.3

a. there was an abundance of text that, ultimately, communicated very little other than a general and high level summary of the relevant position. While WhatsApp has asserted, in this regard, that there is no aspect of Article 13 in relation to which no information has been provided, I respectfully observe that it does not necessarily follow that the provision of text results in the actual communication of the required information;

b. there was an over-supply of linked material that, for the most part, presented a variation of the generalised information that had previously been presented at the first layer. Insofar as that linked material might have provided additional *prescribed* information, it was difficult to clearly identify the information of significance given that it was mixed in with generalised information that was similar to that which had been provided at the first layer. In some instances, the path provided by the links was actually circular;

c. the language used to describe the purpose of any processing was so high level that it is more appropriately described as information that identifies general processing initiatives, e.g. "to promote safety and security". Such an approach communicates nothing, in terms of enabling the data subject to understand how his/her personal data will be processed and the specific objectives sought to be achieved by that processing;

d. information was frequently presented in a piecemeal fashion, whereby information on a particular topic, for example, the period for which the personal data will be stored, has been scattered across different sections and documents. In some instances, the information provided in one location contradicted that provided in another location;

e. certain key information has been set out in an entirely separate notice with only a single link from the body of the Privacy Policy. This was the case, for example, with the Facebook FAQ. This was surprising, given the liberal approach to the incorporation of hyperlinks that was evident elsewhere in the Privacy Policy;

f. the language used, in certain respects, was unnecessarily ambiguous, e.g. the information that had been provided in pursuance of compliance with Article 13(1)(f).

621. As a result of the above, the assessment of the material provided took a significant period of time to document and complete. It was a needlessly frustrating exercise that required the extensive and repeated search of the Privacy Policy and related material to try and piece together the full extent of the information that had been provided in relation to any individual category of Article 13. The most frustrating aspect of all was the manner in which WhatsApp formulated its Legal Basis Notice; this document made it impossible for me to understand which legal basis might be relied on for any particular act of processing, as required by Article 13(1)(c). This was because, for the most part, WhatsApp indicated potential reliance on multiple legal bases to ground a generally identified processing initiative. WhatsApp, in its Preliminary Draft Submissions, suggested that, in having adopted such an approach, it was "*being transparent about the fact that it relies on different legal bases in different circumstances, and does not consider this should be a point of criticism*[278]." It is surprising to me that WhatsApp considers this patent ambiguity to represent transparency,

[278] The Preliminary Draft Submissions, paragraph 7.6

particularly given the clear direction and examples set out on pages 8 and 9 of the Transparency Guidelines (as referenced above) on this very issue.

622. I have recorded, in Parts 2 and 3 of the Decision, all of the information that has been provided, by reference to each individual category of information prescribed by Article 13. It is self-evident, from those records, that there is a significant information deficit. The position is exacerbated by the inaccessibility of the information itself; in other words, the level of effort required to access, review and exhaust all possible avenues of information. This aspect of matters is also clearly demonstrated by the assessments recorded in Parts 2 and 3 of this Decision.

623. The fundamental point of the matter is that, despite my best efforts, I did not receive the information that WhatsApp purported to have provided – even by reference to its own interpretations of Article 13. I note, for example, that, even if I am incorrect in my formulation of the Proposed Approach (and, for the record, I do not consider this to be the case), WhatsApp has not even provided the information that it believes Article 13(1)(c) to prescribe. WhatsApp's position, in this regard, is that Article 13(1)(c) requires the provision of information such that there is a link between the purpose of the processing and the supporting legal basis. While WhatsApp's position[279] is that it has provided this information, this is clearly not the case. As summarised above (and recorded in detail as part of the corresponding assessment in Part 2 of this Decision), it is impossible to tell which legal basis will support any general processing initiative because the information provided is vague, contradictory and ambiguous. It is therefore entirely incorrect to characterise the findings proposed in the Preliminary Draft, as "nuanced", such that they might be said to represent findings that WhatsApp should have provided more granular information "in addition to what it currently provides". The findings of infringement, as set out in this Decision, represent a position whereby the prescribed information, in each case save for Article 13(2)(c) (which will be considered further, below), has simply not been provided.

624. Against the background of the above, I further note that Articles 13 and 14 do not permit the provision of "some" of the prescribed information. Rather they require all of the prescribed information to be provided. Therefore, a failure to provide all of the required information will constitute an infringement of the relevant sub-article requirement. I have already considered, in Parts 1, 2, 3 and 4 of this Decision, the significant role and function that transparency plays in the context of the GDPR, as a whole. In these circumstances, I do not agree that it is inappropriate for me to apply a so-called "binary" approach to the outcome of my assessment. The simple fact of the matter is that an incomplete approach to the provision of information undermines one of the data subject's most fundamental data protection rights. The position is no different if the information provided is ambiguous. The infringements found in Parts 2 and 3 of this Decision represent, in all but one instance, serious information deficits, as follows:

    a. Article 13(1)(c) – as set out above, the information provided by WhatsApp left me unable to discern which legal basis it would rely on when processing personal data for a particular purpose. WhatsApp indicated potential reliance on all of the legal bases set out in Article 6(1) and, in many cases, suggested that it could rely on different legal bases to support an identified general processing initiative. The information provided simply does not enable the reader, upon any objective review of the material, to receive the information prescribed by Article 13(1)(c). I further note, in this regard, that WhatsApp has included a legal basis to ground the

[279] The Inquiry Submissions, paragraph 1.6(B)

sharing of personal data with Facebook, in respect of processing that, I now understand, does not actually take place. As already observed, the purpose of Article 13 is to enable the data subject to learn how his/her personal data will be processed in the context of the particular processing that will be carried out by the data controller concerned. WhatsApp's approach to Article 13(1)(c) does not satisfy this objective.

b. Article 13(1)(d) – as set out in the Article 65 Decision, the Board determined that WhatsApp failed to provide the prescribed information in circumstances where the Legal Basis Notice does not specify "*the provided information with regard to the corresponding processing operation such as information about what categories of personal data are being processed for which processing pursued under basis (sic) of each legitimate interest respectively*[280]." The Board further noted[281], in this regard, that the Transparency Guidelines "state that the specific interest in question to be identified for the benefit of the data subject". It further noted[282] "the similarities between the examples of non-transparent ("poor practice") information put forward in the Transparency Guidelines and the Legal Basis (N)otice … which includes for example: "For providing measurement, analytics, and other business services where we are processing data as a controller […]; "The legitimate interests we rely on for this processing are: […] In the interests of businesses and other partners to help them understand their customers and improve their businesses, validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services"." In the circumstances, it is clear that the Board considered that WhatsApp's approach to the Article 13(1)(d) information requirement to be inadequate and not in line with the requirements and guidance set out in the Transparency Guidelines.

c. Article 13(1)(e) – as before, the information provided under this heading was generalised and vague. It suggested that personal data would be shared with service providers and with third parties as part of the delivery of WhatsApp's services. In relation to the former category of recipient, I have already recorded the number of links and texts that must be negotiated in order to access all of the information provided. At the end of this exercise, the use of qualifying language (as already considered in the corresponding assessment in Part 3) leaves the reader questioning what, exactly, is meant by the "Facebook Companies". As regards the potential sharing of personal data with third parties as part of the delivery of WhatsApp's service, it is left to the reader to guess as to what this might mean in reality. Again, this was an issue that was specifically considered in the Transparency Guidelines[283]. The clear directions provided, in this regard, are not reflected in WhatsApp's Privacy Policy and related material.

d. Article 13(1)(f) – the information provided under this heading is such that the reader is informed that relevant transfers will take place but, beyond that, it is not possible to discern anything further about the particular circumstances of the transfers. Again, as an approach, this is completely inadequate. It remains to be seen how WhatsApp considered its approach,

[280] The Article 65 Decision, paragraph 59
[281] The Article 65 Decision, paragraph 52
[282] The Article 65 Decision, paragraph 62
[283] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 37

in this regard, to represent the "meaningful" delivery of information, as required by the Transparency Guidelines[284].

e. Article 13(2)(a) – as before, this requirement was specifically considered by the Transparency Guidelines[285]. Despite the guidance provided, the information provided by WhatsApp is vague and misleading (as clearly explained in the relevant aspect of Part 2). It is unfair to give the reader the clear impression that he/she has the power to determine the retention period for his/her personal data but to undermine that position in other areas of the material with vague information as to the possible retention of personal data in insufficiently explained circumstances.

f. Article 13(2)(c) – I have made a finding, in this regard, that, while WhatsApp has taken steps towards compliance with this provision, those steps were rendered ineffective as a result of the scattering of slightly different information on the subject in three different areas of the Privacy Policy. I noted, in this regard, that the section of the Privacy Policy most likely to be consulted by the data subject, if he/she wishes to learn about his/her data subject rights (the section entitled "How You Exercise Your Rights") does not include any reference to the right to withdraw consent to processing. In these circumstances, the effectiveness of WhatsApp's approach is entirely dependent on which section the data subject visits first and whether or not he/she decides to look for further information in other locations. I observed, in this regard, that, if the data subject located the information in the "Managing and Deleting Your Information" section, he/she would be given to believe that, if he/she wished to withdraw his/her consent to any consent-based processing, he/she would have to delete his/her account (as opposed to simply adjusting his/her device-based settings).

g. Article 13(2)(e) – my assessment under this heading records that it is not clear, from the information provided by WhatsApp, what minimum information must be processed in order to provide the Service. Further, the (possible) consequences of failure to provide data are not clearly set out for the data subject. Indeed, I noted that the only text provided, in this regard, is confusing.

625. Considering, then, the question of whether or not it is appropriate for me to adopt a so-called binary approach to quantify the extent of non-compliance found in the context of this particular inquiry, I note that Article 13(2)(c) requires the data controller to inform the data subject of "the existence" of the right to withdraw consent. While I remain of the view that the placement of this information is such that it might or might not be discovered by the data subject, I acknowledge that WhatsApp's submissions have some merit in this particular context, given that the existence of this particular right has been identified in the Privacy Policy and, accordingly, I will take this into account within my assessment of gravity for the purpose of Article 83(2)(a).

[284] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 38
[285] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), pages 38 and 39

626. Otherwise, I am satisfied that it is appropriate for me to consider that there has been a total failure to provide the information prescribed by Articles 13(1)(c), 13(1)(d)[286], 13(1)(e), 13(1)(f), 13(2)(a) and 13(2)(e). As regards WhatsApp's submission that "*the logic of the Commission's reasoning is that WhatsApp is equally culpable for providing [the text assessed to be insufficient] as it would have been if it had provided no information whatsoever on the relevant topic*", I agree that this is a correct reflection of the position. My view is that the information provided in furtherance of Articles 13(1)(c), 13(1)(e), 13(1)(f), 13(2)(a) and 13(2)(e) is of such limited utility to the data subject that I am unable to agree with WhatsApp's suggestion that "*the essence of the GDPR requirement is adhered to*". The Board made an equivalent determination[287], in relation to the finding of infringement of Article 13(1)(d). To be clear, however, the adoption of such an approach does not create a situation, as WhatsApp appears to suggest, whereby, for the purpose of this Part 5, WhatsApp is in the same position as a data controller that might have made no effort whatsoever to provide the prescribed information. While WhatsApp's efforts did not produce the intended result (i.e. full compliance), I will (as considered further, below) take account of the efforts made, in this regard, within the relevant aspect of the Article 83(2) assessment.

627. As regards my proposed finding that WhatsApp has failed to provide any information to non-users, I note that WhatsApp has submitted[288] that it "*already makes information publicly available on the very limited way in which it engages with non-user data*". The information provided by WhatsApp, in this regard, has been included in the "Information We Collect" section of the Privacy Policy, as follows:

> *"You provide us, all in accordance with applicable laws, the phone numbers in your mobile address book on a regular basis, including those of both the users of our Services and your other contacts."*

628. I do not consider that this statement merits credit, as regards any potential offset against the information that has not been provided to non-users pursuant to Article 14. In terms of the information communicated by the statement, it tells the user that WhatsApp will collect the phone numbers of everyone in his/her mobile address book on a regular basis and that this may include the phone numbers of non-users. It does not contain the required information as to the processing operations that will be carried out on the numbers, the purpose of the processing of non-user numbers or the period for which it will be retained. Most significantly, it does not enable the non-user to understand the way in which he/she will be individually and uniquely affected by the

[286] The Board, at paragraph 59 of the Article 65 Decision, found that "in the Legal Basis Notice [WhatsApp] has not specified the provided information with regard to the corresponding processing operation such as information about what categories of personal data are being processed for which processing pursued under basis (sic) of each legitimate interest respectively. The Legal Basis Notice does not contain such specific information in relation to the processing operation(s) or set of operations involved." The Board further found, at paragraphs 61, 63 and 64 of the Article 65 Decision that "several passages from the Legal Basis Notice … do not meet the necessary threshold of clarity and intelligibility that is required by Article 13(1)(d) GDPR in this case" and that "it is unclear what is meant by "other business services", as [WhatsApp] does not disclose this information or provide a relation to the specific legitimate interest. The [Board] also notes that it is unclear which businesses or partners [WhatsApp] refers to" and, further, that "descriptions of the legitimate interest as the basis of a processing like "[t]o create, provide, support, and maintain innovative Services and features […]" do not meet the required threshold of clarity required by Article 13(1)(d) GDPR, as they do not inform the data subjects about what data is used for what "Services" under the basis of Article 6(1)(f) GDPR, especially regarding data subjects under the age of majority." In paragraph 65, the Board determined that the same applies in respect of the stated interest to "[share] information with the Facebook Companies to promote safety and security". The Board made it clear that it considered the information provided by WhatsApp, under this heading, to be inadequate to such a degree that it hampered the ability of the data subject to exercise his/her data subject rights. Accordingly, partial credit cannot be given, in respect of any information that has been provided in furtherance of Article 13(1)(d).

[287] The Article 65 Decision, paragraph 66

[288] The Preliminary Draft Submissions, paragraph 5.1

processing in the event that he/she decides to join the Service. In the circumstances, I am satisfied that it is appropriate for me to carry out the Article 83(2) assessment by reference to a position whereby there has been a total failure to provide the required information to non-users.

629. For the avoidance of doubt, and insofar as I have identified, by way of any previously proposed directions or *obiter dicta* comments, any other issues that, while requiring improvement, fall outside of the findings of infringement, I have not taken account of any such previously proposed directions or *obiter dicta* comments (or the underlying assessments) in any assessment carried out for the purpose of this Part 5.

*Submissions in relation to WhatsApp's careful and good faith efforts to achieve compliance with the transparency provisions and/or WhatsApp's position that its approach is aligned with the approach adopted by many industry peers and/or WhatsApp's pre-GDPR engagement with the Commission (the "**Careful and Good Faith Efforts Submissions**")*

Alignment with Industry Peers / Industry Practice

630. WhatsApp has submitted[289], in this regard, that:

> *"WhatsApp has always considered, and continues to consider, that it satisfies the transparency requirements set out in the GDPR. Indeed, its approach is aligned with the approach adopted by many industry peers[290]."*

631. I note that I have already set out my views on the possible significance of alignment with industry peers as part of my assessment of WhatsApp's Submissions of General Application in Part 2 of this Decision (by reference to the category of "Submissions concerning Legal Certainty"). The views so expressed apply equally here.

632. As set out above, my view is that the transparency requirements are clearly set out in the GDPR and additional guidance/direction is available by way of the Transparency Guidelines. While it is undoubtedly the case that the style and language of communicating information cannot be optimised for every individual person and the privacy notice is, by its nature, a somewhat "blunt" instrument, nonetheless, it is clear that Articles 12 – 14 of the GDPR require certain basics that are beyond debate. Accordingly, while an industry-wide failure (if this is, in fact, the case) to achieve compliance with the transparency requirements is a poor reflection on that industry, it is not, however, evidence of a position whereby data controllers in this particular sector are unable to identify what is required of them, in terms of transparency. Further, an (alleged) failure to achieve compliance with the transparency obligations, on the part of WhatsApp's industry peers, is not something that could absolve WhatsApp of its own individual responsibility as a data controller given, in particular, the accountability obligation set out in Article 5(2). Accordingly, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to such submissions.

WhatsApp's pre-GDPR engagement with the Commission

[289] The submissions falling under this particular heading are set out in paragraph 1.3, paragraph 2.1, paragraph 5.12 and paragraph 6.4(E) of the Supplemental Draft Submissions
[290] The Supplemental Draft Submissions, paragraph 2.1

633. WhatsApp's submissions[291], in this regard, include the following:

> *"WhatsApp also considers that the Commission should take account of the fact that it was consulted extensively during the process of developing WhatsApp's Privacy Policy and related documents in 2018, and so was made aware of the approach WhatsApp was planning to take in respect of transparency from prior to the relevant user-facing information even being launched[292]."*

634. I note that I have already assessed the substance of this particular category of submissions as part of my assessment of WhatsApp's Submissions of General Application in Part 2 of this Decision (by reference to the category of "Submissions concerning WhatsApp's pre-GDPR engagement with the Commission"). The views so expressed apply equally here. In summary, my view is that it is not appropriate for WhatsApp to seek to make the Commission (even partially) responsible for its compliance with the GDPR. Accordingly, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to such submissions.

Careful and Good Faith Efforts

635. WhatsApp has submitted[293], in this regard, that:

> *"Any administrative fine would be inappropriate, unnecessary and disproportionate in the circumstances where a reprimand has been issued given: …*
>
> *3. WhatsApp's careful and good faith efforts to achieve compliance – in this respect, WhatsApp submits that the Commission's findings in the Supplemental Draft that WhatsApp has "made efforts towards achieving compliance" and that there is a "genuinely held belief, on WhatsApp's part" that "its approach to transparency complies, in full, with the GDPR" are important; …[294]"*

636. I wish to make it clear, by way of response to this particular submission, that no such findings were made by me, either in the Supplemental Draft or otherwise. I recognised, at paragraph 45(d) of the Supplemental Draft, that WhatsApp "has made efforts towards achieving compliance". I noted, in the same sentence, that those efforts fell significantly short of what is required by Articles 12 and 13.

637. In relation to WhatsApp's "genuinely held belief", I recognised this as part of my assessment in the Supplemental Draft of the Article 83(2)(c) criterion, which requires consideration of "any action taken by the controller or processor to mitigate the damage suffered by data subjects". I noted, in this regard, that it would be unfair to criticize WhatsApp for failing to take action to mitigate any damage suffered in circumstances where its position was that no infringement had occurred and, accordingly, no damage had been suffered by data subjects. It was important for me to recognise, at the same time, that WhatsApp is perfectly entitled to maintain such a position, which I accepted as being genuinely held in the absence of any indication to the contrary.

[291] The submissions falling under this particular heading are set out in paragraph 5.18(A), paragraph 6.4(B), paragraph 10.1 and paragraph 12.1
[292] The Supplemental Draft Submissions, paragraph 12.1
[293] The submissions falling under this particular heading are set out in paragraph 1.6, paragraph 3.4(B)(3), paragraph 5.3, paragraph 5.5, paragraphs 6.4(A) and (B), paragraph 7.1, paragraph 8.4 and paragraph 16.6(B) of the Supplemental Draft Submissions
[294] The Supplemental Draft Submissions, paragraph 3.4(B)(3)

638. As is clear from the above, the statements in question were made in particular contexts and it is incorrect to suggest that they have meaning beyond those particular contexts.

639. Otherwise, the substance of WhatsApp's submissions, under this heading, are that:

> *"The Commission … has also failed to take account of WhatsApp's significant efforts to achieve compliance with its transparency obligations and the information it provides to users[295]."*

640. WhatsApp clarifies, in this regard, that:

> *"For example, WhatsApp's pre-GDPR efforts, details of which have previously been communicated to the Commission in the context of this Inquiry … [including] the extensive engagement with the Commission on the GDPR update … WhatsApp's research on transparency (where it conducted independent user-testing of its proposed new user facing information) and the extensive resources that WhatsApp invested in updating its user facing information (which incorporated expert input from Engineering, Product, Policy, Design, Marketing, Communications and User Research departments, in addition to Legal teams)[296]."*

641. It further submits that:

> *"There is no requirement in the GDPR for controllers to engage experts, or carry out research to assess the best approach to provide the information required by Article 13 GDPR, or proactively engage with the Commission in advance of launch. In carrying out this work, WhatsApp considers it exceeded what could reasonably be expected of it in order to seek to meet its GDPR transparency requirements[297]."*

642. I note, in this regard, that Articles 12 – 14 require the data controller to provide the prescribed information. This is the required standard of compliance; not the making of efforts (substantial or otherwise) towards achieving compliance. While I recognise that WhatsApp made efforts towards compliance, the weight that might be attributed to such efforts, as a mitigating factor for the purpose of this Part 5, is somewhat limited in circumstances where (i) those efforts did not produce the intended result, and (ii) the level of non-compliance, as assessed, is significant. I will take account, insofar as possible, of the efforts made within the relevant aspect of the Article 83(2) assessment.

*Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related materials, on a voluntary basis (the "**Willingness to Change Submissions**")*

643. WhatsApp has submitted[298], in this regard, that:

> *"… in light of the interpretations … that the Commission has now articulated, WhatsApp has volunteered … to adapt its transparency documents to meet the Commission's stated expectations, and in fact began planning changes as part of its ongoing consideration of how best to provide transparency in June 2019, when it learned of the preliminary findings of the Inquiry team.*

[295] The Supplemental Draft Submissions, paragraph 5.5
[296] The Supplemental Draft Submissions, footnote 22 (as referenced in paragraph 5.5)
[297] The Supplemental Draft Submissions, paragraph 6.4(B)
[298] The submissions falling under this particular heading are set out in paragraph 1.7, paragraph 3.4(A), paragraph 3.4(B)(4), paragraphs 5.18(B), (C) and (D), paragraph 7.2 and paragraph 10.1

WhatsApp's prompt expression of its willingness to comply with the Commission's newly articulated interpretations of the GDPR transparency requirements further underlines that it is inappropriate, unnecessary and disproportionate for the Commission to take any corrective action (and particularly action of the nature envisaged in the Supplemental Draft) to ensure compliance[299]."

644. It has further submitted that:

"WhatsApp has already volunteered to change the information it provides in order to address the Commission's concerns, after starting to consider such changes as soon as it learned of the Inquiry team's views on transparency and subsequently proposing the detailed changes set out in its Preliminary Draft Submissions (i.e., prior to receiving the Supplemental Draft)[300]".

645. I have already set out the reasons why I do not accept that my assessments and views represent "newly articulated interpretations" of the GDPR transparency requirements. As regards WhatsApp's willingness to amend its approach to the delivery of the prescribed information, I note firstly that, despite WhatsApp's position that it began considering its position in June 2019, it has only just (as of December 2020) begun to implement those changes (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes). While I acknowledge that the making of such changes might entail a certain lead-in time, I note that almost eighteen months has passed since the time WhatsApp started considering its position.

646. While I welcome WhatsApp's willingness to amend its position, on a voluntary basis, I do not agree that such willingness renders the exercise of corrective powers (including the possible imposition of an order to bring processing operations into compliance) inappropriate, unnecessary and/or disproportionate in the circumstances of this particular inquiry. Firstly, the inquiry is based on the state of information available at the commencement of the inquiry and a number of infringements of the transparency provisions are found to have occurred, in that context. A willingness to remedy the cause of the infringements does not preclude corrective action. Secondly, WhatsApp has maintained its position, throughout the inquiry, that, as far as it is concerned, it has fully complied with its obligations pursuant to the GDPR. WhatsApp is perfectly entitled to maintain this position, however, when coupled with WhatsApp's expressed disagreement with certain of the approaches that I have proposed, it creates certain limitations, in terms of the weight that I might attribute to WhatsApp's willingness to change, in the context of the choices that I must make for the purpose of Article 58(2).

647. Against the background of the above, I will take account, as appropriate, of WhatsApp's willingness to change its user-facing material, on a voluntary basis, as part of the relevant assessment(s) for the purpose of this Part 5.

Submissions that the Commission has not demonstrated how WhatsApp's approach to transparency has in fact had any negative impact on data subject rights and/or that the Commission's concerns that the alleged infringements have impacted on data subjects' rights is theoretical and not supported as a matter of fact and/or that the Commission's analysis of the damage allegedly suffered by data subjects is based on assertions rather than evidence / no evidence has been provided to indicate that WhatsApp's approach to

[299] The Supplemental Draft Submissions, paragraph 1.7
[300] The Supplemental Draft Submissions, paragraph 3.4(B)(4)

*providing transparency has undermined the effective exercise of the data subject rights (the **"Theoretical Risk Submissions")***

648. WhatsApp firstly submits[301], in this regard, that the Commission has not demonstrated how its approach to transparency has in fact had any negative impact on data subject rights. With specific reference to the position of users, it submits[302] that:

    a. The issues identified by Parts 2 and 3 of this Decision do not impact on users' ability to make a fully informed decision, based on the information WhatsApp currently provides as to whether they wish to use the Service and for WhatsApp to process their personal data; and

    b. No examples have been provided of how data subjects "may be deprived" of the information they need to exercise their data subject rights, as suggested in the Supplemental Draft.

649. It is clear that, as regards the first limb of WhatsApp's submissions, above, WhatsApp and I fundamentally disagree as to the quality and quantity of the information that has been provided by way of the Privacy Policy and related materials. I have already set out, in detail, the reasons why I consider the information provided to users to be insufficient. The deficiencies identified are such that the user, in my view, cannot make informed decisions in relation to whether or not they wish to continue using the Service (including the Contact Feature) and for WhatsApp to continue processing their personal data, in that context.

650. The second limb of WhatsApp's submissions, above, is directed to challenging my view that the information deficiencies identified in Parts 2 and 3 of this Decision are such that data subjects "may be deprived" of the information they need to exercise their data subject rights. I note, in this regard, that WhatsApp's own Legal Basis Notice expressly recognises the link between the data subject's knowledge as to the legal basis being relied upon and the corresponding rights that might be exercised by the data subject. The relevant statement, which is set out at the very top of the Legal Basis Notice, provides that:

    *"You have particular rights available to you **depending on** which legal basis we use …" [emphasis added]*

651. As recorded in Parts 2 and 3 of this Decision, I have proposed findings that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c). One of the issues arising, in this regard, is that the information, as presented, does not enable the data subject to understand which legal basis will be relied upon by WhatsApp when it processes his/her personal data for a particular purpose. All the data subject knows, from the information presented in the Legal Basis Notice, is that WhatsApp might rely on different legal bases to ground the same general processing activity, depending on the circumstances. This leaves the data subject unable to identify if, for example, he/she is entitled to invoke his/her right to object to the processing of his/her personal data. This right is only enforceable if the processing is grounded upon Article 6(1)(e) or Article 6(1)(f) (and the controller does not have compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims). The information provided by WhatsApp, by way of the Legal Basis Notice, does not, however, enable the data subject

[301] The Supplemental Draft Submissions, paragraph 5.4
[302] The Supplemental Draft Submissions, paragraphs 5.4 and 5.6 (see also paragraphs 5.28 and 5.32)

to identify if any processing operation is grounded upon Articles 6(1)(e) or 6(1)(f) and, accordingly, he/she is unable to identify if he/she is entitled to exercise his/her right to object to processing.

652. Further, if that data subject decides, regardless, to try and invoke the right to object but his/her request is refused on the basis that the processing is not grounded upon Articles 6(1)(e) or 6(1)(f), the data subject has no way of checking this because he/she has never been informed, as part of the collection of the personal data in question, the legal basis that would be relied upon to ground its processing. In this way, the data subject is unable to hold the data controller accountable. Further, the data subject is unable to identify whether or not he/she might have a valid basis for complaint, so as to be able to make an informed decision as to whether he/she might wish to pursue the matter further by lodging a complaint with a supervisory authority.

653. It is therefore clear that the issues identified in Parts 2 and 3 of this Decision are such that the data subjects concerned may be deprived of the information they need to exercise their data subject rights. While I note WhatsApp's submission that users do seek to exercise data subject rights,[303] this does not remedy the issue demonstrated in the example set out above.

654. In relation to the position of non-users, WhatsApp submits[304] that:

a. Even if it were to concede that it has obligations under Article 14, it would be impossible for it to do any more than it currently does to respect non-users' data subject rights. By way of example, WhatsApp explains that it cannot comply with data subject rights requests as a result of the privacy protective technical measures it has implemented to protect the mobile phone numbers of non-users. Accordingly, WhatsApp submits that the concern expressed, that the (proposed) infringement (as it was when set out in the Preliminary Draft) of Article 14 has impacted on non-users' data subject rights, is "theoretical and not supported as a matter of fact"; and

b. To the extent that my concerns arise from an alleged inability, on the part of WhatsApp users to make informed decisions, this is also unfounded. WhatsApp's view, in this regard, is that the statement provided in the "Information We Collect" section of the Privacy Policy enables the user to make an informed decision as to whether or not they wish to use the Contact Feature and allow WhatsApp to access non-user contact information in their mobile address book.

655. In respect of the first limb of WhatsApp's submissions, above, I acknowledge that the circumstances of the processing of non-user data are such that the range of data subject rights that might be exercised by a non-user data subject are limited. They are not, however, non-existent. I firstly note, in this regard, that the right of access enshrined in Article 15 requires the data controller to provide access to the personal data and also furnish a range of specified information to the data subject concerned. By WhatsApp's own account[305], it responds to data access requests from non-users by explaining "the manner in which non-user data is handled". If, in doing so, WhatsApp provides the information prescribed by Articles 15(1) and (2), then, ostensibly, it is complying with its obligations to the non-user data subject concerned pursuant to Article 15.

[303] The Supplemental Draft Submissions, paragraphs 5.31 and 5.32
[304] The Supplemental Draft Submissions, paragraphs 5.8, 5.9 and 5.10 (see also paragraphs 5.28, 5.33 and 5.34)
[305] The Supplemental Draft Submissions, paragraph 5.34

656. I further note that, if WhatsApp were to make the information that it provides to individual non-user data subjects publicly available, this would enable non-users to understand the way in which their personal data have been/might be processed by WhatsApp, in the event that their phone number is contained in the address book of a user who has activated the Contact Feature. This, in turn, would avoid a situation whereby a concerned non-user, seeking to find out more, has no option but to exercise one of his/her data subject rights.

657. The most significant loss of control that results from the proposed Article 14 infringement, however, is in the case of a non-user who is considering joining the Service. If that non-user's mobile phone has been processed by WhatsApp pursuant to the Contact Feature, he/she will appear in the derivative users' contact lists as soon as he/she joins the Service. The non-user has no way of knowing this in advance and is thereby deprived of the ability to (i) make an informed decision about potentially joining the Service; and (ii) exercise control over his/her personal data.

658. As regards the second limb of WhatsApp's submissions, above, my response is the same as that provided at paragraph 651 to 653, above.

659. Finally, I note WhatsApp's submission[306] that I have not explained how Articles 11 and 12(2) of the GDPR impact on my analysis. The short answer to this is that these provisions have no application in circumstances where I have already found that the mobile phone number of a non-user constitutes the personal data of the non-user concerned because he/she can be said to be "identifiable".

660. By way of the Article 65 Submissions, WhatsApp further submitted, under this heading, that:

    a. No evidence has been put forward to support claims of any harm or risk to users or non-users arising from the infringements alleged to have occurred, nor has any evidence been provided that any data subjects would have acted differently if they had been provided with information in the manner prescribed in the Composite Draft. WhatsApp submits, in this regard, that "(i)f anything the lack of any concrete and identifiable harm in this case supports [WhatsApp's] position that the fine at its [then proposed] level is unwarranted and disproportionate."[307]

    b. In relation to non-users specifically, WhatsApp considers the concerns about risk and harm raised by the Commission (and CSAs) to be "unwarranted and based on unsupported speculation"[308]. In WhatsApp's view, "(t)he "harm" described is essentially a restatement that an infringement has occurred – namely, that it is not made clear to a non-user that they may appear in other users' WhatsApp contact lists after the non-user becomes a user. No further step has been taken to articulate the consequence of the information not being provided[309]."

    c. WhatsApp further submits that there is "a significant discrepancy between the processing that gives rise to the alleged infringement of Article 14 GDPR, and the processing which is relied upon as leading to the alleged harm to non-users. Such a discrepancy arises in this case because … (t)he Composite Draft concludes that [WhatsApp] has infringed Article 14 GDPR

[306] The Supplemental Draft Submissions, paragraph 5.33
[307] The Article 65 Submissions, paragraph 39.14
[308] The Article 65 Submissions, paragraph 39.18
[309] The Article 65 Submissions, paragraph 39.18(B)

with respect to a processing operation conducted in relation to one dataset for one purpose (i.e. non-users' phone numbers accessed through the [Contact Feature] and processed to create the lossy hash …), but is then relying on an entirely different processing operation conducted in relation to a different dataset in order to find that harm was caused (i.e. use of a new user's phone number provided after they sign up to the Service in order to generate a notification hash, which is then used to update the contact lists of existing users). As a result, the true position is that the alleged harm relied on in the Composite Draft cannot in fact be attributed to the processing underlying the finding of alleged infringement of Article 14 GDPR. In fact, Article 14 GDPR is not even relevant to the processing operation relied upon as giving rise to the alleged harm, given the data in question (i.e. the new user's phone number) has been collected directly from the data subject once they … have signed up to use WhatsApp and is therefore subject to Article 13 GDPR considerations, in respect of which [WhatsApp] complies. Given the alleged harm does not in fact arise from the alleged infringement, it should not be taken into account when assessing any fine[310]."

d. In addition, any harm to non-users "of the nature alleged would, in any event, be extremely limited for two reasons[311]:

   i. Firstly, a non-user (once they become a user) will only ever appear in an existing WhatsApp user's contact list if the existing user already has the non-user's phone number stored as a contact on their device. The assumption must be that this is generally the result of the non-user previously having shared their phone number with the existing WhatsApp user, in the expectation that they would be contacted by that person. …

   ii. Secondly, according to the Composite Draft, the "harm" to non-users only "crystallises at the point in time when that non-user becomes a user of the Service". However, importantly, at that point in time the non-user … has already been provided with [WhatsApp's] Terms of Service and Privacy Policy … ."

e. WhatsApp also submits[312] that the Commission's assessment of the extent of any "harm" to non-users does not take into account "the fact that [WhatsApp] would be entitled to rely on the following factors, both of which demonstrate the limitations on any harm that can plausibly be said to have been caused to non-users in this case:

   i. Article 14(5)(b) GDPR which, on the facts of this case, means that [WhatsApp] would not be obliged to provide information to non-users directly … and instead could only be required to "take appropriate measures to protect the data subject's rights and freedoms and legitimate interests" (which it does) ... [and]

   ii. Article 11 GDPR which, on the facts of this case, limits [WhatsApp's] obligations to non-users under Articles 15 to 20 GDPR. This is relevant to the question of harm given the Commission has relied on failings in transparency as having inhibited data subject's (sic) ability to exercise their rights under these provisions in its harm assessment. Article 11 GDPR is applicable in this case because … [WhatsApp] only processes such non-users'

[310] The Article 65 Submissions, paragraph 39.18(C)
[311] The Article 65 Submissions, paragraph 39.19
[312] The Article 65 Submissions, paragraph 39.20

> phone numbers for a matter of seconds prior to the [application of the cryptographic hashing process], during which period [WhatsApp] has no mechanism to re-access those unhashed numbers in other ways or to reverse the effects of the process. As such, if this information constitutes personal data of non-users in the manner concluded in the Composite Draft, it must constitute personal data processed for purposes which "do not or do no longer require the identification of a data subject by the controller" (per Article 11(1) GDPR)."

661. In response to the above submissions, I firstly note that 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. In this case, I have (repeatedly and most recently in paragraphs 655 to 657 above) outlined the consequences for the data subject, both user and non-user, of the infringements of the transparency provisions. To be clear about the position, while the risks to the rights and freedoms of the non-user data subject, other than at the point of signing up to use the Service, are somewhat limited, they are not insignificant.

662. Further, WhatsApp is incorrect when it suggests[313] that the Composite Draft provides that the "harm" to non-users "only" crystallises "at the point in time when that non-user becomes a user of the Service". The relevant part of the Decision[314] records that "the unique and individual impact of the processing upon each individual non-user crystallises at the point in time when that non-user becomes a user of the Service." It is at that point that the purpose of the processing of the individual's mobile phone number (when the individual was a non-user), namely, the 'quick and convenient' updating of user contact lists[315], is achieved. This formed part of my assessment in circumstances where WhatsApp submitted[316] that the purpose of the Contact Feature was not to identify non-users. To be clear about the position, the relevant statement was not an assessment of the damage caused to non-users by the processing. That assessment is recorded within this Part 5 (formerly Part 4 of the Composite Draft), where I have clearly identified the loss of control arising, both for non-users generally as well as those on the point of signing up to become users of the Service in paragraphs 655 to 657 above.

663. As regards WhatsApp's submissions concerning the "significant discrepancy between the processing that gives rise to the alleged infringement of Article 14 GDPR, and the processing which is relied upon as leading to the alleged harm to non-users", I do not agree with WhatsApp's position for the following reasons:

[313] The Article 65 Submissions, paragraph 39.19(B)
[314] See paragraph 105, above
[315] The Response to Investigator's Questions
[316] See paragraph 92, above

a. As part of my determination that the mobile phone number of a non-user constitutes the personal data of that non-user, I set out my view[317] that, while I accepted that WhatsApp does not process the mobile phone numbers of non-users for the specific purpose of identifying those non-users, it is clear that the processing is designed to impact upon an individual non-user in the event that he/she subsequently decides to become a user of the Service. In this way, the processing, while not designed to *identify* the non-user concerned, will, nonetheless, have individual and unique impact for the non-user concerned if he/she subsequently decides to become a user. In the circumstances, it is clear that my determination of the matter involved consideration of the impact of the Contact Feature "in the round" as opposed to the artificially segregated manner now being suggested by WhatsApp.

b. I note that this approach is consistent with the approach taken by the CJEU in the Facebook Fan Pages case, in which the CJEU assessed the status of the controllers concerned by analysing the various processing that took place in the context of a fan page. While the Court identified the controllers concerned by reference to their respective abilities to determine the means and purposes of certain aspects of the processing taking place in the context of the fan page, its ultimate determination was that the fan page administrator and Facebook Ireland were joint controllers for the purpose of the processing that took place in the context of the fan page. In other words, the status of controllership was not defined by reference to individual processing operations that were taking place in the context of the fan page, but rather by reference to the processing that was taking place, in the round, by way of the fan page. The fact that the CJEU recognised that "those operators may be involved at different stages of that processing … and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case" does not change the position that the status of (joint) controller was assigned for the purpose of the global (rather than individual) processing operations that were taking place by way of the fan page.

c. For the sake of completeness, I further note that I clarified, at the outset of the Article 83(2) assessments set out below, that "the processing concerned", for the purpose of those assessments, should be understood as meaning all of the processing operations that WhatsApp carries out on the personal data under its controllership. On the basis of the foregoing, I do not accept that I am required to assess the Article 14 infringement by reference only to the processing operations that take place prior to the non-user signing up to become a user of the Service.

664. As regards the submission that is premised on the assumption that the non-user previously shared their phone number with the relevant user "in the expectation that they would be contacted by that person", I do not agree that this is an assumption that I ought to take into account when assessing the damage to non-users. There are any number of ways in which a user might come to have a non-user's mobile phone number in his/her address book, only one of which involves the non-user having provided the number to the user directly, in the expectation that he/she would be contacted by that user. It is possible, for example, that the user was given the non-user's number by a third party. Further, the assumption does not take account of the context in which the number might have been provided by the non-user to the user. It might well have been the case, for example, that the number

[317] See paragraph 92, above

was provided for a specific purpose or in the context of a particular relationship which has since completed/come to an end. In such a case, the non-user might not wish for his/her contact details to appear in the relevant user's WhatsApp contact list in the event of his/her signing up to the Service.

665. I have already addressed WhatsApp's submissions concerning the possible application of the Article 14(5)(b) exemption in Part 1 of this Decision. In relation to WhatsApp's submissions concerning the possible application of Article 11, I remain of the view expressed at paragraph 659 above. In any event, it is important to note that nothing in this Decision requires WhatsApp to "maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation". Further, Article 11(2) only concerns the application of Articles 15 to 20 of the GDPR. It does not impact on the data subject's entitlement to receive the information prescribed by Articles 13 and 14 and neither does it impact on the data subject's right to object pursuant to Article 21 or his/her right to lodge a complaint with a supervisory authority. In the circumstances, I do not agree with WhatsApp's submission that Article 11, were it to be applicable, would have any significant impact on my assessment of the damage caused by the processing for the purpose of this Part 5.

WhatsApp's Article 65 Submissions

666. WhatsApp, by way of its Article 65 Submissions, advanced a number of arguments that have general application to the Article 83(2) assessments set out below. As a procedural economy, and with a view to avoiding unnecessary duplication, I will respond to those submissions within this section only. Thus, where, as part of its response to any assessment of any individual aspect of Article 83, WhatsApp has indicated reliance on any matter covered by the Article 65 Submissions, the views set out below should be understood as being my views on the relevant subject-matter.

667. WhatsApp has firstly expressed concern that "the mitigating factors, in respect of which [WhatsApp] has made extensive submissions, have not been adequately taken into account[318]." WhatsApp submitted[319], in this regard, that "(t)he fact that the Commission has failed to attribute appropriate weight to relevant mitigating factors is demonstrated by the fact that it has not taken into account mitigations in this process even though it has considered those same mitigations to be relevant in other [named] inquiries."

668. As acknowledged by WhatsApp, I have already addressed these concerns by way of letter dated 13 May 2021. That letter explained that the Commission is not required to apply the same approach across all of its inquiries. The Commission's approach to the presence or absence of relevant previous infringements (for the purpose of the Article 83(2)(e) assessment) differs, depending *inter alia* on the contexts of different types of controllers and, in particular, the scale of the processing at issue. Unlike the position with the smaller-scale domestic inquiries that WhatsApp has cited as examples, inquiries into larger internet platforms generally concern data controllers or processors with multi-national operations and significant resources available to them, including large, in-house, compliance teams. Such entitles are further likely to be engaged in business activities that are uniquely dependent on the large-scale processing of personal data. The Commission's view is that the size and scale of such entities, the level of dependency on data processing and the extensive resources that are available to them necessitate a different approach to the absence of previous relevant infringements. That

[318] The Article 65 Submissions, paragraphs 39.23 to 39.28
[319] The Article 65 Submissions, paragraphs 39.24 to 39.27

approach has been reflected in the decisions that have been cited by WhatsApp in support of its submission. I note, in this regard, that WhatsApp's submissions do not reference the Commission's decision in the Twitter (breach notification) inquiry. The Commission's approach to the Article 83(2) assessment, as recorded in the Twitter decision, is consistent with that applied to the within inquiry (and recorded in this Part 5). Against the background of the above, the Commission does not accept that the matters identified in WhatsApp's submission represent inconsistency in the Commission's approach to determining the quantum of any fine.

669. WhatsApp has further referred to the fact that, in the context of certain previously published decisions, the Commission, where it identified a mitigating factor, also quantified the value of that mitigating factor. WhatsApp asked the Commission to adopt the same methodology to the within inquiry. As set out above, the Commission is not required to apply the same approach to the assessment and quantification of a proposed fine across all of its inquiries. In the context, however, of the more granular approach taken in certain of the domestic inquiries for which decisions have been published, the Commission does not agree that the absence of a similar level of granularity, in any other inquiry, constitutes a material difference in approach, as between those inquiries. The reasons why the Commission varies its approach, as between inquiries, are explained above. In the context of the difference in granularity, it is also important to note that the decisions relied upon by WhatsApp all concern public bodies. As WhatsApp is undoubtedly aware, Section 141(4) of the 2018 Act restricts the fine that may be imposed on a public body (that does not act as an undertaking within the meaning of the Competition Act, 2002) to a maximum of €1,000,000. This is also a factor, in terms of the Commission's decision to vary the degree of granularity that it applies to the fining assessment, as between different inquiries.

670. WhatsApp has further submitted[320] that there has been an "over emphasis" on the number of data subjects and that this factor has been afforded "more than appropriate weight" by the Commission. It is important to note, in this regard, that the Board considered, as part of its Article 65 Decision, the weight that was attributed to this particular factor. It determined[321], in this regard, that:

> *"the Draft Decision adequately qualifies the infringements as very serious in terms of the affected number of data subjects and the consequences of the non-compliance in light of the facts of the case. With regard to the assessment of whether the fine is proportionate, effective and dissuasive in light of these elements, the [Board] refers to paragraph 405 and following of the present decision*."

671. The Board further instructed[322] the Commission to "set out a higher fine amount for the infringements identified", to take account of the various determinations made by the Board, as summarised in Section 9.4 of the Article 65 Decision. Section 9.4 includes an instruction requiring the Commission to ensure that the amount of the fine "shall appropriately reflect the aggravating factors identified in the [Composite Draft]" (noting that the number of affected data subjects was treated, in the Draft Decision, as an aggravating factor). The Commission is bound by the Board's decision and, accordingly, I am unable to attribute any further weight to WhatsApp's submissions in relation to the weight attributed to the number of affected data subjects, as a mitigating factor for the purpose of

[320] The Article 65 Submissions, paragraph 39.28
[321] The Article 65 Decision, paragraph 401
[322] The Article 65 Decision, paragraph 424

this Part 5. Otherwise, I am satisfied that I have adequately taken account of any mitigating factors put forward by WhatsApp as part of the Article 83(2) assessments recorded below.

672. WhatsApp has further made submissions concerning the use of (i) the legal maximums set out in Articles 83(4) to 83(6) of the GDPR as well as (ii) turnover to calculate the fine. I note, however, that these matters are the subject of determinations of the Board, as recorded in the Article 65 Decision[323]. Accordingly, the Commission is required to apply the method of calculation determined by the Board when reassessing the proposed fine, for the purpose of this Decision.

673. In relation to WhatsApp's submissions[324] concerning proportionality, I note that these submissions were taken into account by the Board when it determined[325] that "the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount … but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR." That determination was followed by an instruction[326] that the Commission take account of the turnover of the relevant undertaking when reassessing the fine for the purpose of Section 9.4 of the Article 65 Decision.

674. In relation to WhatsApp's submissions under the heading "(u)nsupported assumptions as to deterrence", I will take account of these submissions, insofar as possible, when reassessing the fine further to the instruction of the Board, as set out in Section 9.4 of the Article 65 Decision.

675. Having considered WhatsApp's Submissions on Recurring Themes and its Article 65 Submissions, I will now assess whether or not my findings, as set out in this Decision, merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

Starting Point: Article 58(2)

676. To begin, I note that Recital 129, which acts as an aid to the interpretation of Article 58, provides that *"… 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 ….*" From that starting point, the relevant corrective powers that are available to me, pursuant to Article 58(2), may be summarised as follows:

> "…
>
> (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
>
> …
>
> (d) 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;
>
> …

[323] See the summary set out in Section 9.4 of the Article 65 Decision
[324] The Article 65 Submissions, paragraphs 39.35 to 39.36
[325] The Article 65 Decision, paragraph 412
[326] The Article 65 Decision, paragraphs 423 and 424

(f) to impose a temporary or definitive limitation including a ban on processing;

…

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

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation."

677. In the circumstances of the within inquiry, and with particular reference to the findings set out in this Decision, I consider that the exercise of one or more corrective powers is both appropriate and necessary for the purpose of ensuring compliance with the GDPR. Of the options available to me, as set out above, I consider that a reprimand and an order to bring processing operations into compliance in the terms set out in **Appendix C** hereto would operate, respectively, to:

a. formally identify and recognise the fact of infringement; and

b. bring about the required remedial action.

678. The exercise of the above corrective powers is, in my view, proportionate in circumstances where the proposed measures do not exceed what is required to enforce compliance with the GDPR, taking into account the findings set out in this Decision. (As will be seen from the below, I have also separately dealt with the question of whether to impose an administrative fine and I deal with WhatsApp's submissions in relation to that issue in that separate analysis).

<u>WhatsApp's Response and Assessment of Decision-Maker</u>

679. WhatsApp, by way of the Supplemental Draft Submissions, disagrees with the above. It firstly submits that I have failed to consider whether any proposed measures are "*appropriate, necessary and proportionate"* and that I have failed to apply the principal of proportionality, insofar as I am obliged to *"impose the least onerous measure available … in order to achieve compliance*[327]." WhatsApp further submits, in this regard, that the proposed order to bring processing operations into compliance is unnecessary because WhatsApp has already volunteered to "*promptly make relevant changes to address the Commission's concerns*[328]".

680. I have clearly set out, in paragraphs 677 and 678, above, the reasons why I consider that the imposition of a reprimand and the making of an order to bring processing operations into compliance is both appropriate and necessary in the circumstances of the findings of infringement recorded in this Decision. I have also noted, in paragraph 678, that I consider these measures to be proportionate to the circumstances. I have already given extensive consideration, in Parts 1, 2, 3 and 4 of this Decision, to the significance, utility and function of the transparency obligation in the context of the GDPR as a whole. WhatsApp, in my view (and the view of the Board), has not discharged its transparency obligations. In the circumstances, it is an entirely proportionate response for me to seek to exercise one or more of the corrective powers set out in Article 58(2) of the GDPR.

[327] The Supplemental Draft Submissions, paragraph 2.2 (see also paragraphs 1.8, 2.3, 2.4 and 3.4)
[328] The Supplemental Draft Submissions, paragraph 3.4(A)

681. I have already identified, in paragraph 677 above, the purpose that would be served by the imposition of a reprimand and, separately, the imposition of an order to bring processing into compliance. I consider the imposition of both measures to be the minimum action required to achieve compliance with the GDPR. The imposition of a reprimand, as already observed, will operate to recognise the fact of infringement. The imposition of an order to bring processing into compliance will operate to remedy the identified defects.

682. I do not agree that WhatsApp's expressed willingness to change its user-facing material renders the imposition of an order to bring processing into compliance unnecessary or disproportionate. As already observed, WhatsApp does not accept any failing on its part, as regards the extent to which it has achieved compliance with the transparency obligations; in the circumstances, the only way that I can ensure that the identified defects will actually be remedied is by way of an order, carrying with it the force of law, to bring processing operations into compliance. The imposition of such an order ensures that the required changes will be made, even if WhatsApp disagrees with the nature of any of the changes that are required to be made to its user-facing information or the rationale for same.

683. Separately, I note WhatsApp's submissions that:

> *"WhatsApp agrees with the Commission that Recital 129 GDPR is the appropriate starting point ... However, the Commission only appears to give consideration to these requirements in the Supplemental Draft at paragraph 45(i). Even then, the Supplemental Draft deals with this issue "[f]or the sake of completeness" only, and the Commission's assessment appears to be conducted solely on the basis of the erroneous reasoning that the proposed reprimand and corrective order "lacks real efficacy in terms of its punitive and deterrent effect" so "accordingly" it is appropriate to issue an administrative fine in addition to those measures[329]."*

684. WhatsApp appears to have mistaken the nature of the reference to Recital 129 in paragraph 45(i) of the Supplemental Draft. That particular reference related to my conclusion, arising from my preliminary assessment of the Article 83(2) criteria in the Supplemental Draft, that the imposition of an administrative fine was warranted. As should have been apparent from paragraphs 4 and 5 of the Supplemental Draft, I separately considered the requirements of Recital 129 in the context of my (then) proposal to impose a reprimand and an order to bring processing into compliance.

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

685. The Hungarian and Dutch SAs each raised an objection concerning the content of the order to bring processing into compliance. The order originally appended to the Composite Draft proposed a six month deadline for compliance and did not reference any requirement for WhatsApp to provide information to non-users concerning the retention of personal data (as a consequence of the application of the lossy hashing process and the storage of the resulting hash value in the Non-User List in combination with the derivative user's contact details).

686. 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 mechanism. Having considered the

[329] The Supplemental Draft Submissions, paragraphs 3.1 and 3.2

merits of the Hungarian SA's objection concerning the length of the deadline for compliance, the Board determined[330] as follows:

> *254. "The EDPB recalls Recital 129 GDPR on the exercise of powers by supervisory authorities, which recalls the need to adopt measures that are appropriate, necessary and proportionate in accordance with the circumstances of the case [331].*
>
> *255. The EDPB notes that the HU SA argued that the deadline for compliance suggested in the Draft Decision would not be in line with Recital 148 GDPR and more specifically with the need for the "applicable legal sanction" to be "chosen in a way for it to be effective, proportionate and dissuasive", taking into account the nature, gravity and consequences of the infringement. It can be acknowledged - as highlighted also by WhatsApp IE [332] - that this recital refers primarily to the imposition of penalties, including administrative fines, which should be imposed in addition to, or instead of appropriate measures imposed by the SA.*
>
> *256. Nevertheless, it can also be noticed that Recital 148 GDPR also refers, for instance, to the imposition of a reprimand instead of a fine in case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person. Therefore, the indications provided by this Recital can be relevant for the imposition of corrective measures in general and for the choice of the combination of corrective measures that is appropriate and proportionate to the infringement committed. Additionally, the need for the corrective measures and any exercise of powers by supervisory authorities to be tailored to the specific case is more broadly expressed also by Recital 129 GDPR.*
>
> *257. The EDPB takes note of WhatsApp IE's statement that "compliance with transparency obligations involves considerable challenges, particularly for controllers who have to explain complex data processing to a wide variety of non-expert users in a way that is nonetheless concise, intelligible, and easily accessible. This is particularly acute in WhatsApp Ireland's case given the Service - which involves a variety of highly technical processes - is used by a broad demographic", and that the period for compliance needs to be a time within which WhatsApp can actually comply [333]. WhatsApp IE further adds that "the implementation of changes to its Privacy Policy and other user facing information is an involved and resource intensive process that requires sufficient lead in time for preparing the relevant changes, internal cross-functional engagement as well as of course engagement with the Commission, localisation and translation of the information for countries in the European Region, and implementing technical changes in the WhatsApp app across five different operating systems" [334].*
>
> *258. The EDPB notes that the HU SA's objection refers to the number of data subjects affected and the nature of the infringement, both of which are pertinent to determine the appropriate, necessary and proportionate deadline for the order. In its*

[330] The Article 65 Decision, paragraphs 254 to 263 (inclusive)

[331] Footnote from the Article 65 Decision: Recital 129 GDPR states that : *"[...] 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, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned."*

[332] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 43.4(B).

[333] Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraphs 44.3-44.4; Supplemental Draft Submissions, section 6.4.C

[334] Footnote from the Article 65 Decision: Supplemental Draft Submission, paragraph 19.1.

Draft Decision, the IE SA explicitly considers the significance, utility and function of the transparency obligation, as well as the number of data subjects affected [335]. However, the HU SA's objection emphasises the need to remedy the infringements within a short timeframe in light of their nature, gravity and consequences in terms of restricting the fundamental rights and freedoms of hundreds of millions of EU citizens.

259. In light of the considerable number of individuals affected in the EU, the EDPB shares the concerns of the HU SA as articulated above, highlighting the importance of the interests of the affected data subjects in seeing Articles 12 - 14 GDPR complied within a short timeframe. The EDPB takes note of the challenges highlighted by WhatsApp IE when it comes to implementing changes to its privacy policy, but in light of the circumstances of the case, in particular, due to the type of organisation, its size and the means (including inter alia financial resources but also legal expertise) available to it, finds of primary importance that compliance with transparency obligations is ensured in the shortest timeframe possible. If WhatsApp IE was found to need six months to update its Privacy Policy to implement the LSA's clear and specific requests, the SAs would be expected to allow for much longer time frames for any smaller organisation, which, in the view of the EDPB, is not appropriate and proportionate in view of ensuring compliance with the GDPR.

260. Moreover, in the circumstances of the present case, the EDPB does not see how a compliance period of three months could be considered disproportionate [336].

261. With respect to WhatsApp IE's arguments as to the need for sufficient time to allow "engagement with the Commission", the EDPB notes the IE SA's Draft Decision contains a comprehensive assessment, guidance and commentary, sufficiently clear and precise to allow WhatsApp IE to fulfil its obligations in accordance with the specific provisions on transparency (Articles 12-14 GDPR) and in view of the accountability principle (Article 5(2) GDPR), with a minimum need to interact with the IE SA in order to implement the request.

262. As regards the argument raised by the IE SA, relating to the fact that non-compliance with the order would constitute a separate infringement of the GDPR and would give rise to the risk of further action being taken against WhatsApp IE, although it is true that non-compliance with an order constitutes a separate infringement of the GDPR (in accordance with Article 83(6) GDPR), it is speculative at this stage whether this situation will occur.

263. In light of the above, the EDPB decides that the IE SA is required to amend its Draft Decision to the effect that the period of six months deadline for compliance is reduced to a period of three months."

687. Having considered the merits of the Dutch SA's objection concerning the absence of reference, in the terms of the order to bring processing into compliance that was appended to the Composite Draft, to the requirement for WhatsApp to provide information to non-users concerning the retention of personal data (as a consequence of the application of the lossy hashing process and

[335] Footnote from the Article 65 Decision: The IE SA refers to "the significance, utility and function of the transparency obligation in the context of the GDPR as a whole" in connection with the proposed order, see Draft Decision, paragraph 642. The IE SA makes its assessment on the number of data subjects affected in connection with article 83(2)(a) GDPR, see Draft Decision, paragraphs 663 - 677.

[336] Footnote from the Article 65 Decision: This is in line with the deadline for compliance initially proposed by the IE SA for actions related to user data. IE SA Composite Response, paragraph 102.

the storage of the resulting hash value in the Non-User List in combination with the derivative user's contact details), the Board determined[337] as follows:

> *"With respect to the NL SA objection concerning the amendment of policies that would be necessary for WhatsApp IE to remedy the infringement of Article 14 GDPR, the EDPB directs the IE SA to ensure that the order to bring processing into compliance, to the extent that it covers the infringement of Article 14 GDPR, clearly reflects the expanded scope of the infringement of this provision as described in section* ***Error! Reference source not found.*** *above (i.e. its connection also to non-user data after the application of the Lossy Hashing procedure)."*

688. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), the order to bring processing into compliance, as set out at **Appendix C** to this Decision, now requires WhatsApp to:

    a. provide information to non-users concerning the retention of personal data (as a consequence of the application of the lossy hashing process and the storage of the resulting hash value in the Non-User List in combination with the derivative user's contact details); and to

    b. carry out the required remedial actions, as specified in the order, within three months of the date of service of the order.

Article 58(2)(i) of the GDPR

689. I note that Article 58(2)(i) permits me to consider the imposition of an administrative fine, pursuant to Article 83, "in addition to, or instead of" the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in Section 115 of the Data Protection Act, 2018, which permits the Commission to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2). Article 83(1), in turn, identifies that the administration of fines "*shall in each individual case be effective, proportionate and dissuasive*".

690. Further, when deciding whether or not to impose an administrative fine and the amount of any such fine, Article 83(2) requires me to give "due regard" to eleven criteria. Those criteria, together with my provisional assessment of each, are set out below.

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

691. As noted in Parts 1, 2, 3 and 4 of this Decision, the Board determined the existence of additional findings of infringement of Articles 13(1)(d), 13(2)(e) and 5(1)(a). In addition, it determined that the scope of the Article 14 infringement should be extended. As part of its consideration of the various objections that were raised by the CSAs in response to the administrative fine that was proposed by the Composite Draft (as detailed, further below), the Board instructed the Commission to re-assess its proposed fine in accordance with the various conclusions that were reached by the Board,

[337] The Article 65 Decision, paragraphs 268

including the conclusion that "the identified additional infringements of Articles 5(1)(a), 13(1)(d), 13(2)(e) and the extended scope of 14 GDPR are to be reflected in the amount of the fine[338] … ."

692. 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 findings of infringement of Articles 13(1)(d), 13(2)(e), Article 5(1)(a) and the extended scope of the Article 14 infringement that were established by the Article 65 Decision.

693. As regards WhatsApp's right to be heard in relation to the assessment of the Article 5(1)(a) infringement (which did not appear in the Composite Draft), WhatsApp was provided with copies of all of the objections that formed the basis for the Board's Article 65 Decision and was invited to furnish submissions in relation to all aspects of same. While WhatsApp furnished submissions in response to the status and merits of the Article 5(1)(a) objections, it did not substantively address that aspect of the Italian SA's objection that indicated that the proposed administrative fine should be reconsidered in the event that a finding of infringement of Article 5(1)(a) is recorded in the Commission's final decision. While I note that WhatsApp has submitted[339] that a concurrent finding of infringement of Article 5(1)(a) alongside findings of infringement of Articles 12 – 14 would amount to double punishment for the same conduct, these submissions were already taken into account by the Board[340] in its Article 65 Decision. That being the case, it is not open to the Commission to reach a contrary assessment to that carried out by the Board.

694. In relation to the infringement of Article 13(2)(e), I note that WhatsApp has addressed[341] this in its Article 65 Submissions on the basis that:

    a. "This matter relates to compliance with Article 13 GDPR, which has not been determined to be the "gravest infringement" in this [inquiry] under Article 83(3) GDPR, and so it is not determinative to the issue of the final fine amount;

    b. … the substantive issue cannot be distinguished from issues arising in respect of compliance with Article 13(1)(c) GDPR which has been addressed in the Composite Draft already and subject to a fine;

    c. There is no evidence of harm to users and this is an example of a technical infringement at best, without any real impact on user rights;

    d. A further fine is not required in order for there to be an effective or dissuasive effect since [WhatsApp] has already taken steps … to improve the information provided in the updated Privacy Policy on this issue; and

    e. It would in any event be procedurally unfair to issue an increased fine at this late stage when the Commission has not addressed the issue in the Composite Draft and afforded [WhatsApp] a meaningful opportunity to make submissions."

[338] The Article 65 Decision, paragraphs 423 and 424
[339] The Article 65 Submissions, paragraphs 10.4 and 13.2
[340] The Article 65 Decision, paragraphs 186 and 187
[341] The Article 65 Submissions, paragraph 17.9

695. In relation to the submissions set out at (a), above, the Board has already considered and issued a determination in relation to the interpretation and manner of application of Article 83(3) (as detailed, further below). Similarly, the Board has also determined that: (i) this Decision should record a finding of infringement of Article 13(2)(e); and (ii) the infringement of Article 13(2)(e) should be taken into account when re-assessing the administrative fine. As already noted, the Commission is bound by the findings that were made the Board, as recorded in the Article 65 Decision.

696. As regards the requirement for me to take account of the additional finding of infringement of Article 13(1)(d) and the expanded scope of the Article 14 infringement, I note that WhatsApp's submissions do not address the issue of how such additional/expanded findings should be addressed, in the context of the administrative fine.

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

Preliminary Considerations

697. I note that Article 83(2)(a) requires consideration of the identified criterion by reference to "the infringement" as well as "the processing concerned". Considering, firstly, the meaning of "infringement", it is clear from Articles 83(3)-(5), that "infringement" means an infringement of a provision of the GDPR. In the context of the within inquiry, I have found that WhatsApp has infringed Articles 5, 12, 13 and 14. Thus, "the infringement", for the purpose of my assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Article 5, an infringement of Article 12, an infringement of Article 13 or an infringement of Article 14 of the GDPR. While each is an individual "infringement" of the relevant provision, they all concern transparency and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, I will assess all four infringements simultaneously, by reference to the collective term "**Infringements**", unless otherwise indicated.

698. It is further important to note that there is a significant degree of overlap, as between the subject-matter of the Article 12 – 14 infringements and the Article 5 infringement. This is clear from the rationale supporting the Board's determination of the existence of the Article 5 infringement (as set out in paragraphs 195 – 199 of the Article 65 Decision). That being the case, the considerations and assessments set out below, save where otherwise indicated, should be understood as being assessments of the individual Article 83(2) criteria in the context of WhatsApp's approach to transparency generally (encompassing both the general principle set out in Article 5 and the more particular obligations arising by reference to Articles 12 – 14).

699. The phrase "the processing concerned" should be understood as meaning all of the processing operations that WhatsApp carries out on the personal data under its controllership. The within inquiry was not based on an assessment of the extent to which WhatsApp complies with its transparency obligations in the context of specific processing operations. Instead, the inquiry examined the extent of the information WhatsApp provides to data subjects about all of the processing operations that it carries out on personal data under its controllership.

700. From this starting point, I will now assess the Article 83(2)(a) criterion in light of the particular circumstances of the within inquiry. I note, in this regard, that Article 83(2)(a) comprises four elements, as follows:

The nature, gravity and duration of the infringement

701. In terms of the **nature** of the Article 12 – 14 infringements, the findings concern infringements of the data subject rights. As set out in the analysis that supported the "Proposed Approach" for the purpose of the Article 13(1)(c) assessment in the Preliminary Draft, my view is that the right concerned – the right to information – is the cornerstone of the rights of the data subject. Indeed, the provision of the information concerned goes to the very heart of the fundamental right of the individual to protection of his/her 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. If the required information has not been provided, the data subject has been deprived of the ability to make a fully informed decision as to whether or not he/she wishes to become a user of the Service. Further, the extent to which a data controller has complied with its transparency obligations has a direct impact on the effectiveness of the other data subject rights. If the data subject has not been provided with the prescribed information, he/she may be deprived of the knowledge he/she needs to consider exercising one of the other data subject rights. Indeed, he/she may even be deprived of knowing about the very existence of the data subject rights.

702. In terms of the Article 5 infringement, the Board observed[342] that transparency "is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive." It is therefore clear that failure to comply with the transparency principle has the potential to undermine other fundamental data protection principles, including but not limited to the principles of fairness and accountability.

703. I further note, in this regard, that Articles 83(4) and (5) are directed to the maximum fine that may be imposed in a particular case. The maximum fine prescribed by Article 83(5) is twice that prescribed by Article 83(4). The infringements covered by Article 83(5) include infringements of the data subject's rights pursuant to Article 12 to 22 as well as the basic principles for processing pursuant to Article 5. It is therefore clear that the legislature considered the data subject rights and the basic principles for processing to be significant, in the context of the data protection framework as a whole.

WhatsApp's Response and Assessment of Decision-Maker

704. By way of response to the above assessment of the Article 12 – 14 infringements, WhatsApp has made submissions that fall within the categories of the Binary Approach Submissions, the Careful and Good Faith Efforts Submissions and the Theoretical Risk Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes set out at paragraphs 599 to 665. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under the Binary Approach Submissions. While I will take account of the matters covered by the Careful and Good Faith Efforts Submissions, it is not appropriate for me to do so in the context of my assessment of the nature of the Infringements. Otherwise, I have addressed the submissions arising under the Theoretical Risk

[342] The Article 65 Decision, paragraph 192

Submissions by providing examples and further reasoning as to the risks arising from the Infringements.

705. In terms of the **gravity** of the Infringements, I note that WhatsApp has not addressed its Article 14 obligations to non-users at all. This means that none of the prescribed information has been provided to non-users of the Service. In the context of users, my provisional findings were such that, in the Supplemental Draft, I considered WhatsApp to have only provided 55%[343] of the prescribed information to users of the Service. As noted above, the Board determined the existence of additional infringements of Articles 13(1)(d) and 13(2)(e). This means that, in total, WhatsApp has been found to have only provided 36%[344] of the prescribed information to users of the Service. This, in my view, represents a very significant level of non-compliance, particularly in the case of the Article 14 infringement, taking into account the importance of the right to information, the consequent impact on the data subjects concerned and the number of data subjects potentially affected (each of which is considered further, below).

706. Turning to the infringement of Article 5(1)(a), the Board determined[345] that there has been "an infringement of the transparency principle under Article 5(1)(a), in light of the gravity and the overarching nature and impact of the infringements, which have a significant negative impact on all of the processing carried out by [WhatsApp]". That being the case, it is clear that the Board did not consider the Article 5 infringement to be insignificant, in terms of gravity.

WhatsApp's Response and Assessment of Decision-Maker

707. By way of response to the above assessment of the Article 12 – 14 infringements, WhatsApp has made submissions that fall within the categories of the Binary Approach Submissions, the New and Subjective Views Submissions, the Nuanced Nature of Assessment Submissions and the Theoretical Risk Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under the New and Subjective Views Submissions and the Nuanced Nature of Assessment Submissions. Further, I have already addressed the submissions arising under the Theoretical Risk Submissions by providing examples and further reasoning as to the risks arising from the Infringements.

708. As regards the Binary Approach Submissions, I have already acknowledged that WhatsApp's submissions have some merit in relation to the proposed finding of infringement of Article 13(2)(c) only. Accordingly, I will adjust my assessment of the extent to which WhatsApp has achieved with its obligations pursuant to Article 13 to reflect a position whereby it has provided 41%[346] of the prescribed information to users of the Service. This assessment gives credit to WhatsApp, as regards its having provided information concerning the *existence* of the right to withdraw consent. As noted

[343] Article 13 sets out twelve categories of information that must be provided to data subjects. The Preliminary Draft records proposed findings that WhatsApp has complied with its obligations in respect of six of the twelve categories. Discounting the applicability of one category (Article 13(2)(f)), the figure of 55% represents the extent to which WhatsApp has achieved compliance with the requirements of Article 13 (i.e. (6/11) x 100).
[344] This figure reflects the additional findings of infringement of Articles 13(1)(d) and 13(2)(e), as established by the Board in its Article 65 Decision. Discounting, as before, the applicability of one category (Article 13(2)(f)), the figure of 36% represents the fact that WhatsApp has been found to have complied with its obligations in respect of four of the eleven prescribed categories (i.e. (4/11) x 100).
[345] The Article 65 Decision, paragraph 199
[346] This reflects an adjustment to the existing formula as follows: (4.5/11) x 100

in my assessment, the placement of this information is such that it might or might not be discovered by the data subject. I have therefore reassessed the extent to which WhatsApp has complied with its Article 13 obligations by reference to the addition of 50% credit for the information that it has provided further to Article 13(2)(c). As explained, as part of my assessment of the Submissions on Recurring Themes, I am not prepared to afford similar credit to WhatsApp in respect of the other proposed findings of infringement in circumstances where I am strongly of the view that the extent of information provided, in each case, was wholly insufficient.

709. In terms of the **duration** of the Infringements, the Privacy Policy bears a "last modified" date of 24 April 2018. Accordingly, it seems to me that the Infringements have been occurring since before the entry into force of the GDPR (and, I note, remain ongoing). For the purpose of this assessment, I will only take account of any period of infringement occurring from 25 May 2018 onwards.

WhatsApp's Response and Assessment of Decision-Maker

710. By way of response to the above aspect of assessment, WhatsApp has made submissions (directed to the assessment of the Article 12 – 14 Infringements) that fall within the categories of the Careful and Good Faith Efforts Submissions, the Willingness to Change Submissions and (indirectly) the New and Subjective Views Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised as part of my assessment of the duration of the Infringements.

Taking into account the nature, scope or purpose of the processing concerned

711. I note that the processing of personal data by WhatsApp, in the context of both users and non-users, is not extensive. In the context of users, WhatsApp processes a limited number of categories of personal data[347], the vast majority of which are expressly furnished by the data subjects concerned. I further note that WhatsApp does not appear to process special categories of personal data. The data are processed in connection with the provision of the Service to users.

712. In the context of non-users, WhatsApp appears to only process, as a controller, the mobile phone numbers of non-users. As before, the data of non-users is processed in connection with the provision of the Service to users. I note, in this regard, that the duration of the processing itself is very short, lasting only a couple of seconds, culminating with the application of a lossy hashing process and the irretrievable deletion of the original mobile phone number. I note, however, that this (albeit limited) processing takes place "on a regular basis[348]" while the Contact Feature is activated on any individual user's device. While WhatsApp submits that it has no ability to access the mobile phone number during the processing and further that it has no practical ability to link the non-user's mobile phone number to a person (or, otherwise, link the resulting Lossy Hash with a specific phone number of an individual non-user), the Board has determined[349] that the "table of lossy hashes together with the associated users' phone numbers as Non-User List constitutes personal data". Following this determination, the Board noted[350] that: *"(t)he only aspect that needs to be assessed is whether, as a consequence of the conclusion concerning the nature of the non-user data after the application of the*

[347] See the "Information We Collect" section of the Privacy Policy
[348] The "Information We Collect" section of the Privacy Policy
[349] The Article 65 Decision, paragraph 156
[350] The Article 65 Decision, paragraph 228

Lossy Hashing procedure, the infringement of Article 14 GDPR extends to such data, too, and whether this needs to be reflected in the choice of corrective measures and amount of the administrative fine." The Board concluded[351] that it "*agrees with the CSAs' objections that the infringement of Article 14 GDPR extends as well to the processing of non-users' data in the form of Non-User Lists after the Lossy Hashing procedure was applied, and instructs the [Commission] to amend its [Composite Draft] accordingly*." On the basis of this instruction, I have reinstated those aspects of my initial Article 83(2) analysis which were premised on a proposed finding that the mobile phone number of a non-user, after the application of the lossy hashing process, remains the personal data of the non-user concerned. Accordingly, I note that, while a limited amount of non-user personal data is processed by WhatsApp, it nonetheless appears to be stored indefinitely on WhatsApp's servers.

713. Overall, it appears clear that the nature and scope of the processing is limited. The purpose of the processing is directed towards achieving connectivity for users. I note, in this regard, that the processing only serves the interests of users and WhatsApp. I acknowledge the "*extensive technical measures which were designed by WhatsApp to ensure this data … is stored and used in a highly privacy protective manner*[352]". In terms of the weight that might be attributed to this factor, however, I note that it does not operate to mitigate against the infringement of the right to be informed, particularly in relation to the consequences of that processing that only crystallise for the non-user concerned, after he/she has signed up as a user of the Service.

As well as the number of data subjects affected

714. In terms of the number of data subjects affected, WhatsApp confirmed[353] that, as at 29 April 2020, it was the controller for approximately [redacted] data subjects in the EEA and the United Kingdom[354].

715. Placing this figure in context, I note that Eurostat, the statistical office of the European Union[355] confirms that[356], as of 1 January 2020:

    a. The population of the "EU-27" was approximately 448 million;
    b. The population of the UK was approximately 67 million[357];
    c. The population of Iceland was approximately 364,000;
    d. The population of Liechtenstein was approximately 39,000; and
    e. The population of Norway was approximately 5 million.

716. By reference to the Eurostat figures, above, it appears that, as at 1 January 2020, the total population of the EEA (including the UK) was approximately 520 million. While it is not possible, or indeed necessary, for me to identify the precise number of users affected by the Infringements, it is useful to

[351] The Article 65 Decision, paragraph 229
[352] The Supplemental Draft Submissions, paragraph 5.16
[353] By way of letter dated 1 May 2020 from WhatsApp to the Commission
[354] The letter dated 1 May 2020 explained, by way of footnote 1 thereto, that: "(t)his figure is based on monthly active users of the Service in the EEA and the United Kingdom. An "active user" is defined as a user that has opened their WhatsApp application at least one time within a given period of time, for example, a month. A monthly active user is defined as a user that has opened their WhatsApp application at least one time in the last 30 days."
[355] https://ec.europa.eu/info/departments/eurostat-european-statistics_en
[356] https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001&plugin=1
[357] This figure has been taken into account, notwithstanding the intervening departure of the UK from the European Union, in circumstances where, as at the date of commencement of the within inquiry, UK-based data subjects fell within the affected scope of data subjects concerned by the cross-border processing in question.

have some point of reference in order to consider the extent of EEA data subjects that are potentially affected by the Infringements. The figure provided by WhatsApp ([redacted] monthly active users) equates to approximately [redacted] of the population of the EEA (including the UK), by reference to the Eurostat figures, above.

717. In terms of the number of non-users affected by the Article 14 infringement, it is not possible for me to identify the number of data subjects concerned. This number, however, cannot be discounted as being potentially insignificant. I observed, in the Supplemental Draft, that, if it is the case that roughly [redacted] of the EEA population are users of the Service, this means that roughly [redacted] of the population are non-users of the Service. All that is required for a non-user's data to be processed by WhatsApp is for that non-user to have his/her contact details stored in the address book of a user. While it cannot be assumed that all of the non-users have been included in the address books of users, I note the comment of the Investigator in the Inquiry Report[358] that, "*there appear to be few barriers to using the [Service] from a socio-economic perspective, aside from the requirement of a user to have a smart device upon which the App can be downloaded.*" On this basis, the number of non-users affected by the Infringement is likely to be significant.

WhatsApp's Response and Assessment of Decision-Maker

718. WhatsApp, by way of the Supplemental Draft Submissions, has responded that:

> *"WhatsApp accepts that there are a large number of users of the Service, and that those users are likely to have chosen to upload device contact lists containing a large number of non-users' phone numbers … However, WhatsApp submits that the number of users can only be relevant … if this can be linked to damage caused to those users …[359]"*

719. I have already addressed, as part of my assessment of the Theoretical Risk Submissions, the risks arising from the proposed Infringements and the consequent non-material damage (loss of control over personal data and the inability to make a fully informed decision) that flow from that.

720. In relation to my assessment of the number of data subjects affected, WhatsApp has submitted, firstly, that:

> *"… WhatsApp should clarify that the number of data subjects in the EEA and the UK previously provided [redacted]) is better understood as an upper bound rather than a specific number, as the figure is based on active phone numbers rather than individual users, and includes WhatsApp business accounts.*
>
> *Further, individuals may have multiple phone numbers registered to the Service. … WhatsApp does not require users to provide identifying information, such as their real name or email address, to create an account. As a result, WhatsApp is not in a position to refine this figure to remove any duplication (i.e. where a number of active phone numbers correspond to the same data subject or correspond with both a business and personal account)[360]."*

[358] The Inquiry Report, paragraph 170
[359] The Supplemental Draft Submissions, paragraph 5.25
[360] The Supplemental Draft Submissions, paragraph 5.26

721. Further information, in relation to the above submission, has been provided by way of a footnote, as follows:

> *"A WhatsApp business account may be operated by a verified business or a private individual user. Further, a single phone number can be linked to both a personal WhatsApp account and a WhatsApp business account, which WhatsApp counts as two accounts[361]."*

722. I will make two observations in response to the above submissions. Firstly, I asked WhatsApp, by way of letter dated 24 April 2020, to confirm:

> *"whether or not I am correct in my understanding that WhatsApp is the data controller for approximately 300 million EEA data subjects."*

723. The response received, dated 1 May 2020, advised that:

> *"As at 29 April 2020, [WhatsApp] is the controller, as defined by Article 4(7) GDPR, for approximately* [redacted] *data subjects in the EEA and the United Kingdom."*

724. As noted above, an accompanying footnote explained that this figure is based on monthly active users of the Service in the EEA and the UK. In other words, the figure represents the number of users that opened their WhatsApp app at least once within the previous 30 days.

725. I acknowledge WhatsApp's submissions that the calculation of the number of users is not an exact science. It is not necessary, for the purpose of the within assessment, for the number of data subjects to be calculable as an exact science. It is sufficient for me to operate by reference to a clear indication as to the sizes of the groups of affected data subjects.

726. By way of second observation, I note that the information required to assess this particular aspect of matters can only be obtained from WhatsApp. This information is uniquely within WhatsApp's control and there is no other source from which I might procure same. While WhatsApp has provided me with a definite figure (albeit an "upper bound") of [redacted], it has not offered any indication of the extent to which this figure might include the variable factors[362] referenced in the Supplemental Draft Submissions. Accordingly, I have no option but to proceed with this particular aspect of my assessment by reference to a figure of [redacted] users, noting that this represents an indication of the size of the affected pool of user data subjects, rather than a specific confirmation of the numbers affected.

727. WhatsApp has further submitted that:

> *"Additionally, the Commission's conclusion that, if roughly* [redacted] *of the relevant population are users of the Service, roughly* [redacted] *are non-users of the Service is … overly-simplistic. For example, the Commission does not give consideration to the various categories of non-users who are unlikely to be listed as contacts in any user's address book. Infants, children and many elderly people do not have mobile phones (and so will not have a mobile phone number) and so are likely to incorrectly account for a material proportion of the Commission's estimated number of "non-users" allegedly*

[361] The Supplemental Draft Submissions, footnote 40 (as referenced in paragraph 5.26)
[362] The Supplemental Draft Submissions, paragraph 5.26

affected. Eurostat figures show that of the population of the "EU-27" approximately 15% are aged 0-14 years and approximately 20% are aged 65 and over. To further illustrate this, research in the UK shows that 12% of 64 – 74 year olds and 25% of 75+ year olds do not use a mobile phone[363]. The Commission's estimation does not take factors such as these into account[364]."

728. As set out above, it is not necessary, for the purpose of the within assessment, for the number of data subjects to be calculable as an exact science. It is sufficient for me to operate by reference to a clear indication as to the size of the group of data subjects affected. WhatsApp has submitted that the rough calculation of the percentage of the relevant population that are likely to be non-users (which derives from the percentage of the population that are likely to be users) does not take account of the various categories of non-users who are unlikely to be listed as contacts in any user's address book. I acknowledge that WhatsApp's submissions have some merit in this regard, and I have adjusted my assessment of the approximate numbers of data subjects affected, as follows:

    a. Taking the Eurostat figures originally referenced (in paragraph 715, above), the total population of the EEA (including the UK) is approximately 520 million.

    b. WhatsApp submits that 15% of the population are aged 0-14 years and so should be discounted from the calculation on the basis that they are unlikely to own a mobile phone and are thereby unlikely to have a mobile phone number that could be processed pursuant to the Contact Feature.

    c. I note, in this regard, that research[365] carried out by the same UK body relied upon by WhatsApp suggests that 45% of children and young adults, between the ages of 5 and 15 years of age, own their own smartphones.

    d. It follows, therefore, that approximately 55% of children and young adults between the ages of 5 and 15 years do not own their own smartphone. Accordingly, the reduction to be applied, by reference to this particular category of individuals, is 43 million (i.e. 55% of 15% of the total EEA population).

    e. WhatsApp further submits that 20% of the population are aged 65 years and over and the percentage of those who do not own a mobile phone, within this age category, varies by reference to a two sub-divided age ranges. The Eurostat figures are not broken down in such a way that would enable an assessment by reference to the age categories specified. For this reason, I have decided to give WhatsApp the maximum benefit possible by assessing this reduction by reference to the higher of the two non-mobile-phone-owner rates specified (i.e. the rate of 25% non-ownership, which applies to those aged 75 years and over).

    f. Accordingly, the reduction to be applied, by reference to this category of individuals, is 26 million (i.e. 25% of 20% of the total EEA population).

[363] Cited Source: Ofcom 'Adults' Media Use & Attitudes Report 2020' available at https://www.ofcom.org.uk/__data/assets/pdf_file/0031/196375/adults-media-use-and-attitudes-2020-report.pdf
[364] The Supplemental Draft Submissions, paragraph 5.27
[365] Ofcom "Children and parents: Media use and attitudes report 2019", available at https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

g. The result of the above is that, of the total population figure of 520 million, approximately 69 million individuals (or 13%) are neither users nor non-users because they are unlikely to own a mobile phone (and so cannot have a mobile phone number to be processed pursuant to the Contact Feature). As before, the user figure provided by WhatsApp (of [redacted] monthly active users), represents approximately [redacted] of the total population of the EEA (including the UK). The corresponding figure, in respect of non-users, however, is reduced to [redacted].

The level of damage suffered by them

729. I note that Recital 75 (which acts as an aid to the interpretation of Article 24, the provision that addresses the responsibility of the controller), describes the "damage" that can result where processing does not accord with the requirements of the GDPR:

> *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: … **where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data** …"* [emphasis added]

730. As set out above, my provisional findings are such that users have only been provided with 41% of the information they are entitled to receive. Non-users have not been provided with any of the information they are entitled to receive. This represents, in my view, a very serious information deficit and one which, by any assessment of matters, can only equate to a significant (in the case of users) and total (in the case of non-users) inability to exercise control over personal data. I further note that, in the case of users, the failure to provide all of the prescribed information undermines the effectiveness of the data subject rights and, consequently, infringes the rights and freedoms of the data subjects concerned.

731. The loss of control over personal data is likely, in my view, to be particularly objectionable to any non-user who might have actively decided against using the Service on the basis of privacy concerns. I note, in this regard, that the European Commission, in its assessment of the (then) proposed acquisition of WhatsApp by Facebook[366], recorded that:

> *"… after the announcement of WhatsApp's acquisition by Facebook and because of privacy concerns, thousands of users downloaded different messaging platforms, in particular Telegram which offers increased privacy protection."*

732. It further recorded[367] that:

> *"Privacy concerns also seem to have promoted a high number of German users to switch from WhatsApp to Threema in the 24 hours following the announcement of Facebook's acquisition of WhatsApp[368]."*

---

[366] European Commission Case No. COMP/M.7217 – Facebook/WhatsApp, dated 3 October 2014 (available at: https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf). See, in particular, paragraph 132 and footnote 79 thereof.
[367] Ibid, paragraph 174
[368] The source of this statement was identified, per footnote 96 of the European Commission's merger decision, as being http://techcrunch.com/2014/02/21/bye-bye-whatsapp-germans-switch-to-threema-for-privacy-reasons/ ; http://www.sueddeutsche.de/digital/seit-facebook-deal-whatsapp-konkurrent-threema-verdoppelt-nutzerzahl-1.1894768

WhatsApp's Response and Assessment of Decision-Maker

733. By way of response to the above aspect of assessment (as it was originally set out in the Supplemental Draft), WhatsApp has made submissions that fall within the categories of the Theoretical Risk Submissions and the Binary Approach Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. I have already taken account of the information that WhatsApp provides in furtherance of Article 13(2)(c) and I have addressed the submissions arising under the Theoretical Risk Submissions, by providing examples and further reasoning as to the risks arising from the Infringements.

734. WhatsApp has further submitted, in relation to the latter, that:

> "*Recital 75 GDPR provides that "the risk to the rights and freedoms of natural persons, of* ***varying likelihood and severity****, may result from personal data processing which could lead to physical, material or non-material damage, in particular … where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data." (emphasis added). WhatsApp submits that the Commission has not adequately considered the varying likelihood and severity of any damage that might possibly be suffered. WhatsApp does not consider there is a likelihood of a data subject suffering damage, let alone significant damage, in the circumstances of this case*[369]."

735. In terms of the likelihood and severity of the identified risks to the rights and freedoms of natural persons, I have already set out my view that the identified risks are the consequence of WhatsApp's failure to provide the prescribed information to users and non-users. In terms of likelihood of the identified risks resulting, therefore, my view is that the identified risks materialise when WhatsApp embarks upon the processing of the personal data concerned without having provided the prescribed information to the data subjects concerned. In terms of the severity of those risks, I have already set out my view that the risks are likely to have a more severe impact for non-users, particularly non-users who might be considering joining the Service, who will not have been provided with any information as to the consequences of the possible processing of their mobile phone numbers, further to the activation of the Contact Feature by any existing user contacts, that will crystallise upon their joining the Service. In the case of users, the identified risks are less severe however I am satisfied that they are appropriately classified as severe given that they concern the infringement of one of the core data subject rights.

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

736. 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 EDPB, in its former composition as the Article 29 Working Party ("the **Working Party**") considered this aspect of matters in its "Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679[370]" ("the **Fining Guidelines**"), as follows:

[369] The Supplemental Draft Submissions, paragraph 5.29

[370] The Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, adopted 3 October 2017, 17/EN WP 253 ("the **Fining Guidelines**")

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

737. Considering, firstly, the Article 12 and 13 infringements, I note WhatsApp's submissions in relation to the efforts that it had made to achieve compliance with its transparency obligations[371].

738. Considering, secondly, the Article 14 infringement, I note that WhatsApp Inc. was previously the subject of a joint investigation carried out by the Office of the Privacy Commissioner of Canada ("**OCO**") and the Dutch Data Protection Authority (College bescherming persoonsgegevens) ("the **CBP**") in 2012 ("the **2012 Investigation**"). I note, in this regard, that WhatsApp is the wholly-owned subsidiary of WhatsApp Inc[372]. I further note that, while, the 2012 Investigation considered this issue by reference to Dutch and Canadian national law, the applicable legal principles (certainly in the case of CBP's investigation) were materially identical to those arising in the context of the GDPR.

739. The resulting investigation reports[373] confirm that the 2012 Investigation included an assessment of whether or not the processing of non-user data collected by way of the Contact Feature was supported by an appropriate legal basis. The CBP's "Report on the definitive findings[374]", in this regard, concluded that the mobile phone numbers of non-users constituted the personal data of the non-users concerned. The CBP observed that a mobile phone number "*is a personal data item because it is a direct contact data item that anyone can use to identify a person directly or indirectly by taking intermediate steps*".

740. It seems to me that, as a result of the findings of the 2012 Investigation, WhatsApp was on notice (via its parent company) that the Dutch Supervisory Authority considered the mobile phone number of a non-user to constitute personal data and that WhatsApp, when processing this personal data pursuant to the Contact Feature, it acted as a data controller.

WhatsApp's Response and Assessment of Decision-Maker

741. In response to the above point, WhatsApp firstly submits that:

"… the Commission's position appears to be predicated on the assumption that an infringement must be either intentional or negligent. WhatsApp submits that this is not the case[375]."

742. There is no doubt but that an infringement may be classified as intentional, negligent or neither intentional nor negligent. I do not, however, consider that the Infringements could appropriately be classified as being neither negligent nor intentional in the circumstances of the within inquiry. Transparency is not only one the core data subject rights, it is also one of the fundamental principles of processing set out in Article 5. This means that data controllers must pay particular care and

[371] The Inquiry Submissions, paragraphs 1.3, 2.5, 2.6 and 10.3
[372] As confirmed by WhatsApp in its letter dated 1 May 2020 to the Commission. See also page 3 of the Directors' Report and Financial Statements most recently filed, on behalf of WhatsApp, with the Companies Registration Office (in respect of the financial period from 6 July 2017 to 31 December 2018).
[373] Available at: https://autoriteitpersoonsgegevens.nl/en/news/canadian-and-dutch-data-privacy-guardians-release-findings-investigation-popular-mobile-app
[374] "Dutch Data Protection Authority Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc. Z2011-00987 Report on the definitive findings", dated January 2013 [Public Version]
[375] The Supplemental Draft Submissions, paragraph 6.2

attention to the requirements of Articles 12 – 14. There is nothing to suggest that the proposed Infringements were the result of intentional behaviour (by way of act or omission) on the part of WhatsApp. My view, however, is that the Infringements suggest a degree of carelessness on WhatsApp's part. The reasoning for this view is set out as part of my assessment, above, of the New and Subjective Views Submissions, the Nuanced Nature of Assessment Submissions and the Binary Approach Submissions.

743. While I recognise, in this regard, that WhatsApp has made efforts towards achieving compliance, it does not necessarily follow that those efforts preclude the possibility of the Infringements being classified as negligent. The fundamental obligation arising, pursuant to Articles 12 – 14, is the provision of information. The extent of non-compliance, as established in Parts 1, 2, 3 and 4 of this Decision, is such that a significant amount of information has simply not been provided. In these circumstances, the efforts made by WhatsApp have limited weight, as a mitigating factor for the purpose of this Part 5 (my views, in this regard, are set out as part of my assessment of the Careful and Good Faith Efforts Submissions). In the context of the within aspect of assessment, I am not satisfied that they can be afforded such weight as to reduce the classification of the Infringements from negligent to neither negligent nor intentional.

744. WhatsApp has further submitted that the Article 12 and 13 Infringements "cannot reasonably be regarded as negligent (or careless)" by reference to submissions falling with the categories of Careful and Good Faith Efforts Submissions, the New and Subjective Views Submissions and the Nuanced Nature of Assessment Submissions. I do not agree with WhatsApp, for the reasons set out within my assessment of the Submissions on Recurring Themes.

745. In relation to the Article 12 and 14 Infringements, WhatsApp objects to my conclusion that this aspect of matters "*demonstrates a high degree of negligence as regards WhatsApp's obligations to non-users*". It further objects to the inclusion of reference to "materials from the 2012 Investigation". It submits[376], in this regard, that:

    a. "*As a purely procedural matter, this is not appropriate given findings in the 2012 Investigation were not previously raised as part of the Inquiry process*"; and

    b. "*In any event, the 2012 Investigation occurred eight years ago in relation to a different data controller (WhatsApp Inc.), pre-dated the GDPR, and was notably before the ruling in Breyer on which the Commission expressly relies on in this Inquiry*."

746. WhatsApp considers[377], in this regard, that:

    "the Commission's reliance on the 2012 Investigation is misplaced and … should be disregarded entirely by the Commission … . Given this misplaced reliance on the 2012 Investigation, the Commission's provisional finding of negligence in relation to the alleged Article 14 Infringement is without foundation and similarly must be reversed[378]."

[376] The Supplemental Draft Submissions, paragraph 6.5(A), (B) and (C)
[377] It is further important to note that the Board took account of this submission (in circumstances where WhatsApp included it in its Article 65 Submissions) when determining the objections raised by the CSAs in relation to the characterisation of the infringements. See paragraph 381 of the Article 65 Decision, in this regard.
[378] The Supplemental Draft Submission, paragraph 6.6

747. While I accept that the significance of the outcome of the 2012 Investigation was not previously put to WhatsApp prior to it being given the opportunity to respond to same as part of the Supplemental Draft, this is because it was not relevant to the examination of the extent to which WhatsApp has complied with its obligations pursuant to Articles 12 – 14. As previously explained[379] to WhatsApp, the role of the investigator is limited to infringement only; he/she is not entitled to consider or make recommendations concerning the proposed exercise of corrective powers. Given that the 2012 Investigation is only relevant to the considerations arising in this Part 5, it could only have been put to WhatsApp as part of the Supplemental Draft.

748. As regards WhatsApp's submissions[380] in relation to the relevance of the findings of the 2012 Investigation to the within assessment, I acknowledge that it may well be the case that the hashing process described in the reports of the 2012 Investigation may be different to that assessed in the context of the within inquiry. To be clear, however, the significance of the findings of the 2012 Investigation, in this regard, is that WhatsApp was on notice (via its parent company) of the fact that both the OCO and CBP considered the mobile phone number of an individual to constitute the personal data of that individual.

749. While I note that the 2012 Investigation occurred eight years ago and predated both the GDPR and *Breyer*, it is nonetheless appropriate for me to have regard to it, particularly in relation to the status of a non-user mobile phone number. I note, in this regard, that the concept of personal data has not changed, as between the Directive and the GDPR. Further, it is irrelevant that it predated *Breyer* in circumstances where the basis for the CBP's conclusion appears to be materially identical to the one recorded in Part 1 of this Decision (while I have considered the application of *Breyer*, as part of the relevant assessment, this was for the sake of completeness only). I do not agree that the difference is such that I cannot have regard to the 2012 Investigation. WhatsApp Inc. is WhatsApp's parent company and, in these circumstances, WhatsApp ought to have known of the position and of its significance in the context of the continued operation of the Contact Feature.

750. Finally, and to be absolutely clear about the position, the relevant aspect of the 2012 Investigation is only significant insofar as it suggests that WhatsApp ought to have known (via its parent company) that an EU data protection authority, operating within the previous EU data protection framework, considered the mobile phone number of a non-user to constitute personal data. In terms of the weight that I have attributed to this, that weight is limited only to my assessment of whether or not the Infringements might appropriately be classified as negligent. My view, as set out above, is that, quite aside from the issue of the 2012 Investigation, the extent of non-compliance found suggests a degree of carelessness (i.e. negligence) on the part of WhatsApp. The impact of the relevant aspect of the 2012 Investigation on this assessment is that I consider the degree of carelessness (negligence) arising to be at the higher end of the scale. As already observed, my view is that the inclusion of transparency as part of (i) the Article 5 data processing principles; and (ii) the data subject rights necessitates particular care and attention on the part of a data controller. In WhatsApp's case, it has fallen particularly short in respect of its obligations to non-users. My view is that it ought to have known, from the outcome of the 2012 Investigation, that its views, as to the status of non-user numbers, would likely not be endorsed by a data protection authority. In these circumstances, it is

[379] By way of the letter dated 19 February 2020 from the Commission to WhatsApp
[380] The Supplemental Draft Submissions, paragraph 6.5

questionable why it did not err on the side of caution and include more information, in relation to the manner of operation of the Contact Feature, in its Privacy Policy. I note, in this regard, that WhatsApp already provides additional information to non-users, on request (i.e. in response to any non-user attempting to exercise a data subject right. For the avoidance of doubt, I have not assessed the extent of information so provided and, accordingly, nothing in this Decision should be understood as acceptance of the sufficiency of such additional information that might be provided). Otherwise, I have not had regard to, nor taken account of, the outcome of the 2012 Investigation as part of my assessment of any other aspect of the Article 83(2) criteria.

751. For the avoidance of doubt, I also consider the Article 5 infringement to be negligent in character on the basis that it does not meet the threshold of being intentional in nature (and the extent of non-compliance with the transparency obligation is such that the infringement cannot be characterised as anything less than negligent).

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

752. The purpose of the within inquiry is to determine whether or not WhatsApp's approach to transparency satisfies the requirements of the GDPR. WhatsApp's position is that its approach to transparency complies, in full, with the GDPR. Notwithstanding my disagreement with this position, I accept that it represents a genuinely held belief, on WhatsApp's part. On this basis, it would arguably be unfair to criticize WhatsApp for failing to take action to mitigate the damage suffered as a result of the Infringements, particularly where WhatsApp's position is that no infringement has occurred and, accordingly, no damage has been suffered by data subjects.

WhatsApp's Response and Assessment of Decision-Maker

753. WhatsApp has submitted[381] that I have not provided any evidence that could support a finding that damage has been suffered by data subjects. I have already addressed, as part of my assessment of the Theoretical Risk Submissions, the risks arising from the proposed Infringements and the consequent non-material damage (loss of control over personal data and the inability to make a fully informed choice) that flows from that.

754. WhatsApp further submits[382] that I have not had due regard to the substantial efforts undertaken by WhatsApp to achieve compliance. I have already considered the substance of these submissions, as part of my assessment of the Careful and Good Faith Efforts Submissions. I am unable to attribute weight to such matters, as a mitigating factor for the purpose of this particular aspect of assessment, in circumstances where this assessment is directed to the action taken to mitigate the damage suffered (the focus of the Careful and Good Faith Efforts Submissions is on the efforts made by WhatsApp to achieve compliance, i.e. the efforts made prior to infringement).

755. It further submits[383] that I have not considered WhatsApp's proposed actions to address the issues raised in the Preliminary Draft Submissions or the fact that WhatsApp volunteered to take such actions as soon as it became aware of the expectations which the Commission has articulated during the course of the within inquiry.

[381] The Supplemental Draft Submissions, paragraph 7.1
[382] The Supplemental Draft Submissions, paragraph 7.1
[383] The Supplemental Draft Submissions, paragraph 7.2

756. I have already explained, as part of my assessment of the New and Subjective Views Submissions, the reasons why I do not agree that the views expressed in Parts 2 and 3 of this Decision can properly be described as 'newly articulated'. In relation to WhatsApp's proposed actions to address the issues raised, I can, and will, later in this Part 5, attribute weight to WhatsApp's willingness to amend its Privacy Policy and related material, on a voluntary basis. I further note, in this regard, that WhatsApp has taken steps beyond merely volunteering to change, in that it has already amended the relevant material. In terms of the weight that may be so attributed, it is limited by reference to (i) my view that there is no reason why WhatsApp could not have properly formulated its Privacy Policy and related material on the basis of the text of Articles 12 – 14, as supported by the Transparency Guidelines; and (ii) WhatsApp has only just (as of December 2020) begun to implement those changes (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes).

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

757. The Fining Guidelines provides, in this regard, 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."*

758. I note that, as regards all four Infringements, while WhatsApp made some effort to communicate the prescribed information to its users, it made no such effort in the context of non-users on the basis that it processed non-user data, as a processor, on behalf of its users. I further note that WhatsApp does not appear to have made any effort to communicate its position to its users such that they could consider their responsibilities as alleged controllers (it is important to note, in this regard, that I have not made any determination as to whether or not an individual user might properly be classified as a data controller, in this context). This lack of communication was an unfortunate oversight given that the users in question signed up for, and used, the Service as consumers, rather than business users, and are unlikely to have anticipated that WhatsApp considered them to be the data controllers of non-user data.

WhatsApp's Response and Assessment of Decision-Maker

759. WhatsApp has submitted[384] that any criticism of its failure to inform non-users that it processes non-user data, as a processor on their behalf, such that they might consider their responsibilities as alleged (or potential) controllers, is inappropriate in circumstances where its users are exempt from the application of the GDPR "due to the household exemption at Article 2(2)(c) GDPR". WhatsApp has submitted, in this regard, that it would be inappropriate for WhatsApp to inform users that they have any obligations under GDPR when they do not.

760. My view on this is that a determination as to whether or not the "household exemption" can be said to apply to the processing carried out, by way of any individual user, cannot be made in the absence of an assessment of the circumstances of processing in the particular case. In note, in this regard,

[384] The Supplemental Draft Submissions, paragraph 8.1

that the exemption only applies where the processing is carried out by a natural person "in the course of a purely personal or household activity". While I accept that, for the most part, this is indeed likely to be the case, it cannot be said that it will apply in each and every case. It is possible, for example, that some individuals might use the Service to communicate with groups in connection with their work or, otherwise, to help organise events on behalf of a club. By informing users of WhatsApp's position (and, again, I emphasise that I am by no means endorsing such a position, that being a separate matter which does not fall for determination in these circumstances), it ensures that the users concerned are made aware of the position such that they might consider whether they have GDPR responsibilities or not. In the circumstances, I disagree that it is inappropriate for me to criticise WhatsApp for failing to have made its position clear, in this regard.

761. WhatsApp has further submitted that the Privacy Policy does provide information to users about how it processes non-user data. My views, in this regard, are already set out as part of my assessment of the Binary Approach Submissions. In summary, I am of the view the information provided is wholly insufficient.

762. WhatsApp further relies on the "*extensive technical measures which were designed by WhatsApp to ensure this data (i.e. non-user contacts uploaded from user' devices) is stored and used in a highly privacy protective manner*[385]". As set out above, the issue for determination, under this heading, is the extent to which the controller *"did what it could be expected to do"*. While it is clear that WhatsApp has implemented measures to help protect the personal data during the course of processing (and I have taken this into account as part of my assessment of the Article 82(2)(a) criterion), such measures do not address its transparency obligations to non-users. In the circumstances, I am unable to attribute weight to this, as a mitigating factor in this particular context.

763. WhatsApp also submits that account should be taken of "*the efforts it undertook to comply with its transparency obligations*" which, it suggests, "*exceed what was required of a controller and aligns with the approaches adopted by industry peers*". My views, on both of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes, set out at paragraphs 599 to 665, above. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to any submissions made on the basis of parity with industry peers or industry standards. I have also set out my views, as part of my consideration of the Careful and Good Faith Efforts Submissions, as to the extent of weight that might be attributed to this particular factor, in the context of this Part 5. I have already taken account of such matters as part of my assessment of Article 83(2)(c). My view is that it is not appropriate for me to give weight to that particular factor within this particular aspect of the Article 83(2) assessment.

<u>Article 83(2)(e): any relevant previous infringements by the controller or processor</u>

764. There are no such previous infringements by WhatsApp under the GDPR.

WhatsApp's Response and Assessment of Decision-Maker

765. WhatsApp submits[386] that the fact that it has never infringed the GDPR must be taken into account as a mitigating factor. I disagree with this suggestion. The Article 83(2) criteria are simply matters

[385] The Supplemental Draft Submissions, paragraph 8.3
[386] The Supplemental Draft Submissions, paragraph 9.1

that I must consider when deciding whether to impose an administrative fine and, if so, the amount of that fine. The Article 83(2) criteria are not binary in nature, such that, when assessed in the context of the circumstances of infringement, they must be found to be either a mitigating or an aggravating factor. The position is similar, in this regard, to the position advanced by WhatsApp in response to my assessment of Article 83(2)(b).

766. Accordingly, it does not follow that the absence of a history of infringement must be taken into account as a mitigating factor. This is particularly the case where the GDPR has only been in force for a relatively short period of time. On this basis, my view is that this is neither a mitigating factor nor an aggravating one for the purpose of the within assessment.

767. By way of the Article 65 Submissions, WhatsApp further sought to rely on (what it considered to be) an inconsistency in the approach taken by the Commission to this particular criterion in other of the Commission's inquiries[387]. I have already addressed those submissions at paragraphs 668 and 669, above.

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

768. The Fining Guidelines provide, in this regard, that:

> *"… it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspection."*

769. While WhatsApp has cooperated fully with the Commission at all stages of the within inquiry, it is required to do so by law. Further, I note that the cooperation that would be relevant to the assessment of this criterion is cooperation "*in order to remedy the infringement and mitigate the possible adverse effects of the infringement*". In the circumstances, nothing arises for assessment by reference to this criterion.

WhatsApp's Response and Assessment of Decision-Maker

770. WhatsApp firstly disagrees that its cooperation during the course of inquiry is not something that may be taken into account under this heading. My position on this is as already outlined. Further, as set out above, within the Article 83(2)(e) assessment, it is not the case that each individual assessment of the Article 83(2) criteria must result in a position whereby the output of the assessment must conclude whether the particular matter applies as a mitigating factor or an aggravating factor.

771. WhatsApp has made further submissions that fall within the categories of the Careful and Good Faith Efforts Submissions, the Willingness to Change Submissions and the New and Subjective Views Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under the New and Subjective Views Submissions or any aspect of the Careful and Good Faith Efforts Submissions that concern WhatsApp's pre-GDPR engagement with the Commission.

[387] The Article 65 Submissions, paragraphs 41.3(C) and 39.27

772. I can, however, take account, as a mitigating factor, of WhatsApp's willingness to change its relevant policies and the fact that it has already taken active steps, to that end. I note that those steps are directed towards remedying the Infringements so it is appropriate that I take them into account here. As to the weight that I might attribute to this, as a mitigating factor, I am somewhat limited by the fact that WhatsApp has only just (as of December 2020) begun to implement those changes (and, for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes).

773. By way of the Article 65 Submissions, WhatsApp further sought to rely on (what it considered to be) an inconsistency in the approach taken by the Commission to this particular criterion in other of the Commission's inquiries[388]. I have already addressed those submissions at paragraphs 668 and 669, above.

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

774. As set out above, the categories of personal data concerned are not extensive and do not include any special category data. In the case of non-users, the processing is limited to a mobile phone number (which, when converted to a Hash Value, is stored in the Non-User List in conjunction with the details of the derivative user[389]).

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

775. The matters giving rise to the Infringements became known to the Commission as a result of an own-volition inquiry. The subject matter of these Infringements did not give rise to any obligation for WhatsApp to make a formal notification to the Commission.

WhatsApp's Response and Assessment of Decision-Maker

776. WhatsApp submits that the fact that the within inquiry is of an own-volition nature "*should have no bearing on whether to impose an administrative fine or on the amount of the proposed fine, particularly in the circumstances of this Inquiry*[390]".

777. In reflecting that this is an own-volition inquiry, as part of my assessment in the Supplemental Draft, I was making the point that the circumstances of (the then proposed) Infringements did not give rise to any obligation, on the part of WhatsApp, to notify the matter to the Commission. As before, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. My view is that nothing arises for consideration under this heading; in other words, this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment.

778. WhatsApp has made further submissions that fall within the categories of the Careful and Good Faith Efforts Submissions (directed to WhatsApp's pre-GPDR engagement with the Commission only). I

[388] The Article 65 Submissions, paragraphs 41.3(D) and 39.26
[389] I note, in this regard, the Board's determination, as recorded in paragraph 156 of the Article 65 Decision, that the Hash Value, when stored in the Non-User List in conjunction with the details of the derivative user, constitutes personal data.
[390] The Supplemental Draft Submissions, paragraph 12.1

have already explained the reasons why I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised.

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

779. No such measures have previously been ordered against WhatsApp.

WhatsApp's Response and Assessment of Decision-Maker

780. WhatsApp has submitted[391] that the fact that it has never been subject to a finding of infringement of the GDPR and has never been ordered to take corrective action must be taken into account, as a mitigating factor.

781. As previously explained, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. My view is that nothing arises for consideration under this heading; in other words, this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment. In any event, as I have already referred to above, I do not consider that the practice of industry peers is relevant to the assessment of an individual controller's compliance with its GDPR obligations. Similarly, I have also previously stated my position that, in light of the deficiencies in WhatsApp's approach to transparency, I do not consider that WhatsApp has adhered to the Transparency Guidelines.

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

782. Such considerations do not arise in this particular case.

WhatsApp's Response and Assessment of Decision-Maker

783. WhatsApp has submitted, in this regard, that:

> *"While WhatsApp has not adhered to codes of conduct or certifications (because none exist), WhatsApp considers that its approach to transparency aligns with the approach adopted by industry peers in terms of compliance with the transparency requirements of the GDPR. Moreover, WhatsApp considers that it complies with all published guidance, including the Transparency Guidelines. WhatsApp submits that these matters should be mitigating factors in the Commission's assessment[392]."*

784. As previously explained, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. My view is that nothing arises for consideration under this heading; in

[391] The Supplemental Draft Submissions, paragraph 13.1
[392] The Supplemental Draft Submissions, paragraph 14.1

other words, this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment.

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

785. The relevant considerations arising under this heading are as follows:

a. WhatsApp does not charge users in the context of the Service.

b. The Article 14 infringement relates to the processing of non-user data pursuant to the activation, by users, of the Contact Feature. According to WhatsApp[393], the Contact Feature is a "popular" voluntary feature of the Service. Non-user data is processed by way of the Contact Feature so as to be able to "*quickly and conveniently update [a user's] contacts list on the Service as and when any of those non-users join the Service*[394]." In this way, the Contact Feature envisages, and is directed to facilitating, the continued growth of WhatsApp's user-base.

c. While the continued growth of WhatsApp's user-base will not necessarily result in a direct financial benefit in the form of new subscription fees, it will increase WhatsApp's presence on the market and thereby potentially increase its value. I note, in this regard, the information provided in the Facebook FAQ[395], that:

> *"We can also count how many unique users WhatsApp has … . This will help WhatsApp more completely report the activity on our service,* ***including to investors*** *and regulators."* [emphasis added]

d. The question that arises, therefore, is whether or not a more transparent approach to the data protection issues arising in the context of the Contact Feature would have a positive, negative or neutral effect on the continued growth of WhatsApp's user base. I expressed the view, in the Supplemental Draft, that a more transparent approach to the Contact Feature would represent a risk factor for the continued growth of WhatsApp's user base in circumstances where existing and prospective users might be encouraged, by concerned non-users, to opt for an alternative service that does not process the personal data of non-users.

WhatsApp's Response and Assessment of Decision-Maker

786. In response, WhatsApp submits[396] that the "*reasoning that a more transparent approach would represent a risk factor to the continued growth of WhatsApp's user base is not supported by any evidence, and appears to be based on a number of incorrect assumptions*.". It submits, in this regard, that:

a. No account appears to have been taken of the fact that users themselves are free to choose whether or not to use the Contact Feature as part of the Service.

[393] Response to Investigator's Questions, WhatsApp's answer to question 3
[394] Response to Investigator's Questions, WhatsApp's answer to question 3a.
[395] Available at https://faq.whatsapp.com/general/26000112/?eea=1 (the "**Facebook FAQ**")
[396] The Supplemental Draft Submissions, paragraphs 15.2 to 15.6 (inclusive)

b. "*Moreover, in order to conclude that a significant proportion of non-users have decided not to use the Service on the basis of privacy concerns, and so would be unhappy that WhatsApp processes their data, the Commission has sought to rely on assertions made in a 2014 article on the website techcrunch.com, which itself was re-reporting a single article, focusing on Germany, on the website of Suddeutsche Zeitung. This article asserted that some people may have been looking for alternative messaging services in the days following the announcement on 19 February 2014 that Facebook was acquiring WhatsApp Inc. Contrary to the unsupported assertions contained in these 2014 articles, according to the data retained from this period, WhatsApp has found no statistically significant variation in account registrations in Germany in the days following 19 February 2014. Indeed, when numbers across the EEA and UK are considered it would seem that the announcement of this acquisition coincided with an overall increase in new account registrations*[397]."

c. A footnote to the above paragraph clarifies, in this regard, that *"(w)hile the data retained by WhatsApp does not include data regarding account deletions, WhatsApp's review of registrations from this period show that new use registrations increased immediately following the announcement, to significantly above the average daily registrations for 2014, on 20 February 2014*."

d. WhatsApp further submits that, in any event, such allegations should not have been raised for the first time at the corrective measures decision-making stage.

e. WhatsApp has further made it clear that it intends to improve the "educational information" that it provides to users in relation to the Contact Feature. WhatsApp does not expect this to result in a decline in the number of users, to slow the growth of users or to impact on the value of the business in any way. WhatsApp's position is that, if, in fact, it were to have further explained the manner in which it processes non-users phone numbers via the Contact Feature publicly "(i.e. in addition to what is already said in this respect in its Privacy Policy)", given the highly privacy protective manner of the relevant processing, it is likely that non-users would have been reassured by the way in which their information is processed by WhatsApp. This, WhatsApp submits, "if anything, would have supported the Service's further growth."

787. For the reasons outlined above, WhatsApp's view is that the conclusion originally outlined should be removed.

788. I note that the "conclusion" under challenge was the conclusion that I reached, on a preliminary basis, as regards whether or not a more transparent approach to the data protection issues arising in the context of the Contact Feature would have a positive, negative or neutral effect on the continued growth of WhatsApp's user base. I provisionally concluded that a more transparent approach would represent a risk factor on the basis that existing and prospective users "might be encouraged" by concerned non-users to seek out an alternative service that does not process the personal data of non-users.

[397] The Supplemental Draft Submissions, paragraph 15.3

789. WhatsApp appears to have correlated the above (proposed) conclusion with the article referenced within the Article 83(2)(a) assessment (in the part dedicated to consideration of the "level of damage suffered" by data subjects). The article was referenced, within that aspect of the assessment, to illustrate one way in which a data subject may exercise control over his/her personal data. In the example presented, the data subjects exercised control by choosing an alternative service. The article itself was not taken into account within the Article 83(2)(a) assessment; indeed, it could not possibly have been since it did not concern the within inquiry nor the (then proposed) Infringements.

790. Returning to the matter under assessment, I made no reference whatsoever to the article in my preliminary assessment of Article 83(2)(k). I formed my view on the basis that it is not clear, from the Privacy Policy or related material, that the activation of the Contact Feature will result in WhatsApp processing the mobile phone numbers of non-users. Neither is it clear how, or for how long, WhatsApp will process that data. Most significantly, the consequences, for the non-user, crystallising at the point in time at which he/she has joined the Service are not clearly set out. As WhatsApp has acknowledged, non-users contact it to exercise their data subject rights, from time to time. Some of those individuals, despite having been provided with further information about the processing that takes place on non-user data, have gone on to lodge complaints with supervisory authorities. It is therefore clear that, certainly for a cohort of non-users, the provision of further information, does not satisfy their concerns.

791. WhatsApp has submitted that the provisional conclusion referred to above (which was originally set out in the Supplemental Draft) does not take account of the fact that users themselves are free to choose whether or not to use the Contact Feature as part of the Service. I take it that, by this submission, WhatsApp is suggesting that a user could avail of the Service without activating the Contact Feature. While this is, of course, a possibility, I note that this would limit the user's ability to communicate by way of the Service. In any event, I do not consider this argument to be persuasive in circumstances where there is insufficient information for users concerning the impact of the Contact Feature so as to enable them to make an informed choice as to whether to activate it.

792. Given that I did not reach my conclusion by reference to the article discussed by WhatsApp in its submissions, I do not need to consider those submissions, in this context.

793. As regards the submission that it was the role of the Commission's inquiry team to raise any such "factual allegations", I note that no such allegations were raised as part of my assessment under this heading. Even if this were not the case, however, I have already explained that consideration of the Article 83(2) factors is the sole preserve of the Decision-Maker; it is outside of the scope of the investigator to consider matters beyond the question of whether or not an infringement has occurred/is occurring.

794. I finally note WhatsApp's submission that it intends to improve the "educational information" that it provides to users in relation to the Contact Feature and that, in WhatsApp's view, "it is likely" that non-users would be reassured by the way in which their data is processed by WhatsApp. As already observed, above, and as referred to by WhatsApp in its Supplemental Draft Submissions, there have been cases whereby non-users, having received an explanation from WhatsApp as to the privacy protective manner in which their personal data has been processed, have nonetheless lodged complaints with a supervisory authority. It is therefore clear that, for this cohort of non-users, the provision of additional information has not had the desired reassuring effect. I further question why,

if WhatsApp believes that the provision of this information would not only reassure non-users but also support the Service's further growth, it has not made publicly available the information that it provides to individual non-users upon request.

795. In terms of how I might take account of WhatsApp's submissions, above, I note that our respective positions effectively cancel each other out. Neither I nor WhatsApp can know, until the contingent event has happened, which one of us is correct in our belief as to the likely impact, on the continued growth of the user base, of a more transparent approach to the data protection issues arising in the context of the Contact Feature. For this reason, I will amend my previously proposed conclusion to reflect that I am unable to predict the likely outcome of a more transparent approach on the continued growth of WhatsApp's user base.

796. WhatsApp has further submitted[398] that:

> *"it is incorrect to claim that it was designed for the purpose of growing WhatsApp's user base. For example, the Contact Feature is not used as a way to somehow identify non-users in order to promote WhatsApp's services to them. Instead, it was designed to ensure the best possible experience for existing users."*

797. The relevant assessment did not contain any such claim. The assessment clearly records my view that the Contact Feature "envisages" – which it does – and "is directed to facilitating" – which it also does – the continued growth of WhatsApp's user-base. I further note that the assessment did not contain any suggestion that the Contact Feature might be used to "*somehow identify non-users in order to promote WhatsApp's service to them*". In the circumstances, it is not necessary for me to take account of these particular submissions within my assessment.

798. WhatsApp also considers that I must take account of "*the fact that [WhatsApp] already publicly explains that it accesses non-user data in its Privacy Policy … which in itself undermines the Commission's conclusion in this regard.*" I have already set out my view that the information provided by WhatsApp, in this regard, is wholly insufficient. Accordingly, and for the reasons that are explained further in my assessment of the Submissions on Recurring Themes, I am unable to take account of this submission, as a mitigating factor for the purpose of this aspect of my assessment.

799. Finally, WhatsApp submits that I should take account, as a mitigating factor, of the fact that "no material financial gains were made in relation to the alleged infringements at issue[399]". As previously explained, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. In having departed from my previous assessment and having now reached a conclusion where I am unable to determine the impact that a more transparent approach would have on the continued growth of WhatsApp's user base, my view is that this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment.

[398] The Supplemental Draft Submissions, paragraph 15.7
[399] The Supplemental Draft Submissions, paragraph 15.7

Decision: Whether to impose an administrative fine and, if so, the amount of the fine

800. Having given due regard to each of the Article 83(2) criteria, as set out above, I have decided that an administrative fine is warranted in circumstances where:

a. All four infringements, in my view, are very serious in **nature**. They go to the heart **of** the general principle of transparency and the fundamental right of the individual to protection of his/her 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. In having only provided 41% of the prescribed information to users and none of the prescribed information to non-users, the Infringements (both collectively and individually) concern a very significant information deficit. Accordingly, it is appropriate to classify the Infringements (both collectively and individually) as being severe in **gravity**, with particular reference to the Article 14 infringement.

b. The Article 12 and 13 infringements appear to affect approximately [redacted] of the population of the EEA (equating to approximately [redacted] data subjects). This is a very large figure. While the number of affected non-users is unquantifiable, the high number of users, together with the popularity of the Contact Feature, suggest that the number of affected non-user data subjects is also likely to be extremely high (noting, in this regard, that I have estimated the corresponding percentage of non-users to be approximately [redacted] of the population of the EEA, including the UK).

c. In terms of the effect of the Article 12 and 13 infringements, users are not provided with all of the information that they need in order to be able meaningfully to consider and exercise their data subject rights. In the context of non-users, the result of the Article 14 infringement is that these data subjects have been denied their right to exercise control over their personal data. The impact is particularly severe, in the case of a non-user who might be considering joining the Service in that he/she is further deprived of the ability to make a fully informed choice. This is because no information whatsoever has been provided to inform the non-user of the way in which the processing of his/her mobile phone number, further to the activation of the Contact Feature by a user whose address book includes the mobile phone number of that non-user, will uniquely and individually impact upon him/her, if he/she decides to join the Service. In other words, he/she has no way of knowing that, if his/her mobile phone number has been processed, his/her details will appear in the contact list of any derivative users once he/she joins the Service. I note, in this regard, that, even if these data subjects took a proactive approach and consulted the information that is made available to users by way of the Page, there is nothing in the information furnished to indicate how non-user data will be processed by WhatsApp. Further, there is nothing in the information furnished to indicate that non-user data is subjected to a lossy hashing process and stored on WhatsApp's servers. This loss of control is likely to be particularly objectionable to those non-users who have actively decided against using the Service on the basis of privacy concerns. I further note, in this regard, that this has been the position since 25 May 2018. Again, my view is that, while each of the infringements is serious, the Article 14 infringement is particularly serious in light of the factors discussed above. The Article 5 infringement, as determined by the Board in the Article 65 Decision, must also be deemed to be very serious in nature, given the extent of the information deficit, when considered by reference to both users and non-users.

d. The above assessments take account of the limited nature and scope of the processing in question. I note that, in the case of non-users, technical measures have been implemented to protect the data in question and the processing, while limited in scope and nature, takes place "on a regular basis" and the resulting lossy hash value appears to be stored indefinitely on WhatsApp's servers. I further note that this processing is directed towards enhancing connectivity for users and provides no benefit to the non-user. While I consider the limited nature and scope of the processing to be a mitigating factor, I am unable to attribute significant weight to it given the seriousness of the Infringements, particularly in relation to non-users.

e. In terms of the **character** of the Infringements, my view is that they each ought to be classified as negligent. Such a classification, in my view, reflects carelessness on the part of the controller or processor concerned. While I recognise, in respect of the Article 12 and 13 infringements, that WhatsApp has made efforts towards achieving compliance with obligations arising (I note, for example, that WhatsApp engaged experts and carried out research when considering how best to meet its transparency obligations to users), those efforts did not achieve their objective (i.e. compliance). The shortfall (which I have assessed to be 59% of the information prescribed by Article 13), in this regard, is significant. The requirements of these provisions are not complex: a data controller is simply required to provide the information listed in Article 13 in a clear and transparent manner. For an organisation of WhatsApp's size, reach and available internal and external resources, the failure to achieve the required standard of transparency is, in my view, negligent.

f. As regards the Article 14 infringement, my view is that this demonstrates a high degree of negligence, as regards WhatsApp's obligations to non-users. I note, in this regard, that the 2012 Investigation included an assessment of the issues arising in relation to the processing of non-user data for the purpose of the Contact Feature. I further note the CBP's conclusion that the mobile phone number of a non-user constituted the personal data of that non-user. That ought to have put WhatsApp (via its parent company) on notice that a European data protection authority was unlikely to agree with its position that it does not process personal data relating to non-users. While I acknowledge WhatsApp's submission that it has, at all times, maintained that it does not process such data as a controller, I remain of the view that, in having failed to put its users on notice of its position, WhatsApp has denied its users the ability to consider their responsibilities as alleged (or potential) data controllers.

g. Accordingly, my view is that each of the Infringements should be characterised as negligent, with the Article 14 infringement demonstrating a high degree of negligence, and taken into account as an aggravating factor for the purpose of the Article 83(2) assessment. The Article 5 infringement must also be characterised as demonstrating a high degree of negligence, given the very significant information deficit (for both users and non-users) and its consequent negative impact on the fairness of the processing carried out by WhatsApp on the personal data of both users and non-users.

h. By reference to **Article 83(2)(d)**, my view is that the matters arising under this heading are a further aggravating factor, in the case of non-users, given the total failure to provide the required information. While the provision of 41% of the prescribed information to users

mitigates the position somewhat (in relation to the Article 12 and 13 Infringements only), my view is that WhatsApp fell significantly short of what it might have been expected to do. Given that Article 5 underpins all of the obligations arising pursuant to Articles 12 – 14, it is clear that the matters arising for assessment pursuant to Article 83(2)(d) are a significant aggravating factor in the context of the Article 5 infringement.

i. The only mitigating factors, in my view, are, firstly, the limited **categories of personal data** undergoing processing, particularly in the case of non-users, and, secondly, WhatsApp's willingness to amend its Privacy Policy and related material. I am unable, however, to attribute significant weight to either of these factors, given the overall seriousness and severity of the Infringements (both collectively and individually) and in light of the fact that WhatsApp has only just (as of December 2020) begun to implement changes to its Privacy Policy and related material (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes).

j. For the sake of completeness, I have also considered whether or not the imposition of an administrative fine is appropriate, necessary and proportionate, in the light of Recital 129 of the GPDR, read in conjunction with, amongst others, Article 83. I have already decided to impose a reprimand in conjunction with an order to bring processing operations into compliance in the terms set out at **Appendix C** so as to (i) formally recognise the fact of infringement and (ii) ensure that WhatsApp takes the remedial action required, respectively. This action, however, lacks real efficacy in terms of its punitive and deterrent effect and, accordingly, it is appropriate, necessary and proportionate for me to conclude that a fine should be imposed in addition to those other measures.

801. On the basis of the clear analysis that I have identified and set out above, the nature, gravity and duration of the Infringements and the potential number of data subjects affected, I have decided to impose the following administrative fines:

a. In respect of the infringement of Article 12, a fine of between €30 million and €55 million.

b. In respect of the infringement of Article 13, a fine of between €30 million and €55 million.

c. In respect of the infringement of Article 14, a fine of between €75 million and €100 million.

d. In respect of the infringement of Article 5, a fine of between €90 million and 115 million.

802. In having determined the quantum of the fines proposed above, I have taken account of the requirement, set out in Article 83(1), 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 already discussed above, the Infringements (collectively and individually) are very serious, both in terms of the extremely large number of data subjects potentially affected and the severe consequences that flow from the failure to comply with the transparency requirements (with particular reference to the impact of the Article 14 infringement on non-users).

803. In order for a fine to be "dissuasive", it must dissuade both the controller/processor concerned as well as other controllers/processors carrying out similar processing operations from repeating the

conduct concerned. In this regard, I take account of the fact that the relevant finding of the 2012 Investigation did not dissuade WhatsApp from its position that it does not process non-user data (as a controller or otherwise).

804. As regards the requirement for any fine to be "proportionate", this requires me to adjust the quantum of any proposed fine 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 WhatsApp's user base, the impact of the Infringements (individually and collectively) on the effectiveness of the data subject rights enshrined in Chapter III of the GDPR and the importance of those rights in the context of the GDPR and, indeed, the scheme of EU law, as a whole, which makes the right to protection of one's personal data a Charter-protected and Treaty-protected right.

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

805. For the avoidance of doubt, I have also taken account, as part of my Article 83(1) assessment, of the turnover of the undertaking concerned (as discussed, further below). The Board determined[400], as part of its Article 65 Decision, in considering various objections raised by CSAs as to the application of the criteria under Article 83(1) and 83(2), that "turnover may also be considered for the calculation of the fine itself, where appropriate, to ensure that the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR". The Board's reasoning for this determination was as follows[401]:

> *405. "Article 83(1) GDPR provides that "[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".*
>
> *406. As indicated above, there is a disagreement between the IE SA and DE SA about* ***whether the turnover figure is relevant*** *only to determine the maximum fine that can be lawfully imposed, or whether it is also potentially relevant in the calculation of the fine amount.*
>
> *407. WhatsApp IE's position is that "[the] sole relevance of turnover for the purpose of Article 83 GDPR is to ensure that any proposed fine - once calculated - does not exceed the maximum fining caps set out in Articles 83(4) to (6) GDPR." Furthermore, WhatsApp IE states that "turnover is not a relevant factor to take into account as part of the Article 83(2) GDPR assessment" because this provision "prescriptively lists the relevant factors that can be taken into account and the legislature chose not to include turnover as a specific factor" [402]. WhatsApp IE rejects the notion that "sensitivity to punishment needs to be taken into account and that the fine needs to have a noticeable impact on the profits of an undertaking", as was raised by the DE SA. Moreover, in WhatsApp IE's view "such an interpretation would be contrary to legal certainty as such a precise factor should have been expressly included in Article 83(2) GDPR" [403].*

[400] The Article 65 Decision, paragraph 412
[401] The Article 65 Decision, paragraphs 405 to 412, inclusive
[402] WhatsApp Article 65 Submissions, paragraph 39.31.
[403] WhatsApp Article 65 Submissions, paragraph 39.49-50.

408. 'Turnover' is mentioned explicitly in Article 83(4)-(6) GDPR, in connection with the calculation of the maximum fine amount applicable to undertakings with a total annual turnover in the previous financial year that amounts to more than 500 million EUR (the dynamic maximum fine amount). The aim is clear: to ensure an effective, appropriate and dissuasive fine can be applied to deter even to the largest undertakings. The Guidelines on Administrative Fines state that "[i]n order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU" [404]. The connection is made between the size of the undertaking, measured in terms of turnover, and the magnitude a fine needs to have in order to be effective, proportionate and dissuasive. In other words, the size of an undertaking - measured in terms of turnover - matters.

409. Though it is true that neither Article 83(2) GDPR nor Article 83(3) GDPR refer to the notion of turnover, drawing from this an absolute conclusion that turnover may be considered exclusively to calculate the maximum fine amount is unsustainable in law. Firstly, including a reference to turnover in these provisions is unnecessary, as on the one hand all fines - whether set close to the upper limit or far below it - must be set at a level that is effective, proportionate and dissuasive (cf. Article 83(1) GDPR), and on the other hand the dynamic maximum fine amount sets out the limits within which the SAs may exercise their fining power. Secondly, it would be internally contradictory for the GDPR to introduce a dynamic upper limit to fines, while at the same time prohibiting supervisory authorities from assessing whether a fine might need to be increased or decreased in light of the turnover of a company - again - to ensure it is effective, proportionate and dissuasive (cf. Article 83(1) GDPR).

410. The words "due regard shall be given to the following" in Article 83(2) GDPR by themselves do not indicate the list is an exhaustive one. The wording of Article 83(2)(k) GDPR, which allows for any other aggravating or mitigating factor to be taken into account - even though not explicitly described - supports this view.

411. The application of a dynamic maximum fine amount is not a novelty in EU law, as this is a well-established notion in European competition law. While the EDPB concedes there are differences between both systems, the similarities are such that CJEU case law from the field of competition law may serve to clarify a number of questions on the application of the GDPR. In particular, the EDPB notes that taking into consideration turnover - as one relevant element among others - for the calculation of fines is an accepted practice in the field of competition law [405].

412. In light of all of the above, the EDPB takes the view that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR. The EDPB therefore instructs the IE SA to take this into account in the present case in the context of amending its Draft Decision on the basis of this binding decision."

[404] Guidelines on Administrative Fines, p. 6.

[405] Commission Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, OJ C 210, 1.9.2006, p. 2–5; Lafarge v Commission, (Case C-413/08 P, judgment delivered 17 June 2010), ECLI:EU:C:2010:346, § 102 and the case law cited.

806. I have also taken account of the Board's determination[406] in relation to the CSA objections that were raised concerning the effectivity, proportionality and dissuasiveness of the proposed fine, as follows:

> *413. "As stated in the Guidelines on Administrative Fines, the assessment of the effectivity, proportionality and dissuasiveness of a fine has to "reflect the objective pursued by the corrective measure chosen, that is either to re-establish compliance with the rules, or to punish unlawful behaviour (or both)" [407].*
>
> *414. The EDPB underlines that, in order to be effective, a fine should reflect the circumstances of the case. Such circumstances not only refer to the specific elements of the infringement, but also those of the controller or processor who committed the infringement, namely its financial position.*
>
> *415. Similarly, the EDPB recalls that the CJEU has consistently held that a dissuasive penalty is one that has a genuine deterrent effect . In that respect, a distinction can be made between general deterrence (discouraging others from committing the same infringement in the future) and specific deterrence (discouraging the addressee of the fine from committing the same infringement again) [408]. Moreover, in order to be proportionate the severity of penalties must be commensurate with the seriousness of the infringements for which they are imposed [409]. It follows that fines must not be disproportionate to the aims pursued, that is to say, to compliance with the data protection rules and that the amount of the fine imposed on an undertaking must be proportionate to the infringement viewed as a whole, account being taken in particular of the gravity of the infringement [410].*
>
> *416. Therefore, when determining whether a fine fulfils the requirements of Article 83(1) GDPR, due account must be given to the elements identified on the basis of Article 83(2) GDPR. In this regard, the EDPB notes that, although the Draft Decision contains a detailed assessment on the different elements, it is unclear how those impact the proposed fine. In particular, the EDPB notes that the IE SA refers to the "nature, gravity and duration of the infringement" and "to the potential number of data subjects affected" [411]. In addition, the IE SA considers that the only mitigating factors (ie. the limited categories of personal data and WhatsApp IE's willingness to amend its Privacy Policy and related material) cannot be attributed "significant weight" given the "overall seriousness and severity" of the infringements [412].*
>
> *417. In its objection, HU SA argues that the fine is ineffective, disproportionate and non-dissuasive, since the elements of Article 83(2) GDPR have not been given due regard and that the IE SA cannot rely on the FR SA's decision on Google LLC in order to determine the amount of the fine, given the higher number of data subject affected in the present case. The IE SA clarifies that the FR SA's decision was only considered after the fines were calculated, in order to ensure the overall consistency of the application of the GDPR[413] and underlines the differences between both cases. The EDPB takes note*

[406] The Article 65 Decision, paragraphs 413 to 422, inclusive
[407] Guidelines on Administrative Fines, p. 6.
[408] See, *inter alia,* Judgment of 13 June 2013, Versalis Spa v. Commission, C-511/11, ECLI:EU:C:2013:386, paragraph 94.
[409] See CJEU Judgment of 25 April 2013, Asociaţia Accept, C-81/12, ECLI:EU:C:2013:275, paragraph 63.
[410] Marine-Harvest EU General Court T-704/14, 26 October 2017, ECLI:EU:T:2017:753, paragraph 580.
[411] Draft Decision, paragraph 747.
[412] Draft Decision, paragraph 746.h.i.
[413] IE SA Composite Response, paragraph 95.

of the views expressed by WhatsApp IE, according to which not only the HU SA mischaracterised the IE SA's reliance on the FR SA's decision but any such reliance was not appropriate [414]: while the FR SA's decision was limited to French residents, the scope of the processing at issue was much broader and had a more significant impact on rights and freedoms of data subjects than the one subject to the Inquiry, and included a finding of infringement of Article 6 GDPR in addition to transparency obligations [415]. According to WhatsApp IE, to the extent that the IE SA relies on the FR SA's decision in determining a fine at the higher end of the proposed range, it should be disregarded [416].

418. As stated above, the DE SA also considers that the amount of the fine does not reflect the seriousness of the infringement, in light of the number of data subjects affected. Further, the DE SA also highlighted in its objection the need for the fine to have a "general preventive effect", since the envisaged fine will instead lead other controllers to "conclude that even total disrespect [for] data protection laws would not lead to significant administrative fines".

419. The EDPB takes note of the position of WhatsApp IE, which is that the fine set out in the Draft Decision is excessive and therefore inconsistent with Article 83(1) GDPR [417].

420. The EDPB agrees with the argument of the IE SA on the need to ensure an overall consistency in the approach when imposing corrective measures, specifically regarding fines. To this end, even though consideration of other fines imposed by other SAs may be insightful, the EDPB underlines that the criteria in Articles 83(1) and 83(2) GDPR remain the main elements to be considered when determining the amount of the fine. In the present case, the EDPB notes that the IE SA has considered the infringements very serious in nature, severe in gravity, with particular reference to the Article 14 GDPR infringement and amounting to a high degree of negligence, being the degree of responsibility a further aggravating factor. In addition, the IE SA does not attribute significant weight to any mitigating factor [418]. All these elements shall be given due regard when determining the proportionality of the fine. In other words, a fine must reflect the gravity of the infringement, taking into account all the elements that may lead to an increase (aggravating factors) or decrease of the amount. Likewise, as stated above, the turnover of the undertaking is also relevant for the determination of the fine itself. Otherwise, the objective of attaining fines which are effective, proportionate and dissuasive would not be met.

421. In sum, when considering whether the proposed fine is effective, proportionate and dissuasive, the EDPB has taken into account the turnover of the concerned undertaking, the infringements occurred and the elements identified under Article 83(2) GDPR.

422. Considering the global annual turnover, the infringements found and the aggravating factors correctly identified by the IE SA, the EDPB considers that the proposed fine does not adequately reflect the seriousness and severity of the infringements nor has a dissuasive effect on WhatsApp IE. Therefore, the fine does not fulfil the requirement of being effective, proportionate and dissuasive. In light of this,

[414] WhatsApp Article 65 Submissions, paragraphs 39.46-39.47.
[415] WhatsApp WhatsApp Article 65 Submissions, paragraph 39.47.
[416] WhatsApp Article 65 Submissions, paragraph 39.48.
[417] WhatsApp Article 65 Submissions, 2.5 and throughout the submission.
[418] Draft Decision, paragraph 746.

the EDPB directs the IE SA to amend its Draft Decision in order to remedy the issue identified when it proceeds with the overall reassessment of the amount of the administrative fine, in accordance with section ***Error! Reference source not found.****."*

807. The Board concluded[419] (in section 9.4 of the Article 65 Decision) that:

> *423. "The EDPB instructs the IE SA to re-assess its envisaged corrective measure in terms of administrative fine in accordance with the conclusions reached by the EDPB, namely:*
>
> - *the relevant turnover is the global annual turnover of all the component companies of the single undertaking (paragraph 292);*
> - *the relevant turnover is the one corresponding to the financial year preceding the date of the final decision taken by the LSA pursuant to Article 65(6) GDPR (paragraph 298).*
> - *the relevant turnover is relevant for the determination of the maximum fine amount and also for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive (paragraph 412).*
> - *the amount of the fine shall appropriately reflect the aggravating factors identified in the Draft Decision under Article 83(2) GDPR, to ensure the fine is proportionate (paragraph 404).*
> - *the identified additional infringements of Articles 5(1)(a), 13(1)(d), 13(2)(e) and the extended scope of 14 GDPR are to be reflected in the amount of the fine, as brought up by several CSAs in their objections [420];*
> - *all the infringements identified in the Draft Decision, as well as the additional ones identified in the present decision, are to be taken into account when calculating the amount of the fine, in accordance with the EDPB's interpretation of Article 83(3) GDPR (paragraph 327).*
>
> *424. In light of the above, the EDPB instructs the IE SA to set out a higher fine amount for the infringements identified, in comparison with the administrative fine envisaged in the Draft Decision, while remaining in line with the criteria of effectiveness, proportionality, and dissuasiveness enshrined in Article 83(1) GDPR."*

808. On the basis of the above, and pursuant to both the binding determinations and associated rationale of the Board as required by Article 65(6), I have taken account of the above instruction when re-assessing the administrative fine to be imposed on WhatsApp pursuant to this Decision.

809. When considering the quantum of the fines proposed in the Composite Draft, I also had regard to the cooperation and consistency provisions set out in Chapter VII of the GDPR. The GDPR contains numerous references to the requirement for supervisory authorities to ensure the consistent

[419] The Article 65 Decision, paragraphs 423 and 424

[420] See IT SA Objection, p. 12, which states that the amount of the administrative fine to be imposed should be reconsidered in case the objections pointing to additional infringements were taken on board. Additionally, please see the objections raised by the FR SA, PT SA and the NL SA described in paragraph **Error! Reference source not found.** regarding the impact o n the corrective measures of the consideration of the lossy hashed data as personal data.

application and enforcement of its provisions. To that end, I note that, by way of decision dated 21 January 2019, the French Data Protection Authority (the Commission Nationale de l'Informatique et des Libertés) ("the **CNIL**") imposed a fine of €50 million on Google LLC in respect of infringements of Articles 6, 12 and 13[421] ("the **CNIL Decision**"). The CNIL Decision, to which I have had regard solely for the purposes of the consistency principle, records three specific findings as follows:

810. Finding 1: "*there is an overall lack of accessibility to the information provided by the company in the context of the processing in question*[422]". The issues referenced in the assessment that resulted in this finding included the deciding body's views that:

    a. The information provided was "*excessively spread out across several documents … [with] buttons and links that must be activated to learn additional information … [and the] fragmentation of information*[423]"

    b. "*Some information is difficult to find*", for example "*information relating to personalised advertising and … geolocation*" and "*retention periods*"[424]

811. Finding 2: "*… there has been a breach of the transparency and information obligations as provided for in Articles 12 and 13 …*"[425]. The issues referenced in the assessment that resulted in this finding included the deciding body's views that:

    a. The information provided "*does not allow users to sufficiently understand the particular consequences of the processing for them*[426]". The examples cited include:

        i. "*the description of the purposes pursued*[427]"
        ii. "*the description of the data collected*[428]"
        iii. "*the legal basis of the personalised advertising processing*[429]"
        iv. The lack of clarity as regards the legal basis being relied upon for particular processing operations[430]
        v. "*retention periods*[431]"

812. Finding 3: "*the consent on which the company bases personalised advertising processing is not validly obtained*.[432]" I note that this finding is not relevant to the within inquiry.

813. The CNIL Decision further records the factors taken into account when considering the imposition of a sanction, as follows:

---

[421] "Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC" available at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf ("the **CNIL Decision**")
[422] Ibid, paragraph 103
[423] Ibid, paragraph 97
[424] Ibid, paragraphs 98, 101 and 102
[425] Ibid, paragraph 128
[426] Ibid, paragraph 111
[427] Ibid, paragraph 113
[428] Ibid, paragraph 114
[429] Ibid, paragraph 117
[430] Ibid, paragraph 118
[431] Ibid, paragraph 120
[432] Ibid, paragraph 167

a. In respect of the nature of the infringements, the deciding body noted that Articles 6, 12 and 13 are central/essential provisions that enable people to maintain control of their data[433].

b. In terms of duration, the decision noted that the infringement was ongoing[434].

c. In terms of the number of data subjects affected by the infringement, the decision suggested that "the data of millions of users is processed by the company in this context"[435].

d. In terms of the processing concerned, the decision noted the "*extensive processing operations" taking place*[436].

e. Finally, considering the responsibility of the company, the decision noted that "*in view of the benefits it derives from this processing, the company must pay particular attention … to its responsibility under the GDPR*"[437].

814. In addition to a fine of €50 million, the CNIL further imposed a complementary "*penalty of publicity*"[438].

815. Considering the similarities between the CNIL's Decision and the proposed outcome of the within inquiry, I note that:

a. Both cases concern the infringement of three core provisions of the GDPR.

b. Both cases concern infringements of an ongoing nature.

c. Both cases concern high numbers of data subjects affected by the identified infringements. While the CNIL's Decision does not definitively identify the approximate number of data subjects concerned, it includes indicators as to the potential numbers involved, e.g. "*millions of users*[439]". I note, in this regard, that the CNIL Decision confirmed that, in 2016, "*the operating system totalled 27 million users in France*[440]". For the purpose of providing an approximate point of reference, the population of France, as at 1 January 2016, was approximately 67 million[441]. On this basis, the cited number of French users appears to represent approximately 40% of the French population.

816. By way of distinguishing features, I note that:

a. The processing covered by the CNIL's Decision was more extensive than the processing operations that appear to be carried out by WhatsApp.

[433] Ibid, paragraphs 176 and 177
[434] Ibid, paragraph 178
[435] Ibid, paragraph 181
[436] Ibid, paragraph 182
[437] Ibid, paragraph 188
[438] Ibid, paragraph 189
[439] Ibid, paragraph 181
[440] Ibid, paragraph 4
[441] https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001&plugin=1

b. While the nature of my findings, in relation to the transparency requirements, are materially identical to Findings 1 and 2 of the CNIL Decision, I have found, in this inquiry, that, in the case of non-users, none of the prescribed information has been provided while, in the case of users, only 59% of the prescribed information has been provided. The within inquiry therefore appears to concern a more severe level of non-compliance with the transparency requirements than that recorded in the CNIL's Decision.

c. The number of data subjects potentially impacted by the Infringements in the within inquiry appears to be significantly higher than the numbers alluded to in the CNIL's Decision (this reflects the restricted geographical scope of the CNIL's investigation, which was limited to users based in France). Further, and most significantly, the Article 14 infringement concerns an unquantifiable number of non-users. As set out above, this is a very significant factor for the purpose of the Article 83(2) assessment, both in and of itself, and in terms of its consequential impact on the assessment of the gravity of the Article 14 infringement.

817. I should emphasise that I note the CNIL Decision for the purposes of the consistency principle only. The Decision is based on the evidence and submissions which I have considered, my assessment of the same within the context of the legal framework of the GDPR and the Board findings, as set out in the Article 65 Decision, which I am bound to follow.

818. Accordingly, in the Composite Draft, I confirmed that I was satisfied that the fines originally proposed represented the consistency of approach required by the GDPR. I noted, in this regard, that the fines in respect of the infringements of Articles 12 and 13 did not exceed the level of the fine imposed by the CNIL Decision. While the quantum of the fines proposed in the context of the Article 5 and 14 infringements are significantly higher than that outlined in the CNIL's Decision, this is appropriate in view of the Board's findings which I am bound to follow. The Board noted, in this regard, the extent of non-compliance recorded in the Composite Draft, which included reference to:

a. The total failure to provide any information to non-users;

b. the consequent invalidation of the fundamental right of those non-users to exercise control over their personal data;

c. the fact that the personal data of non-users is being processed by WhatsApp without their knowledge and possibly against their wishes;

d. my views as to the highly negligent character of the Article 14 infringement, noting, in particular, the outcome of the 2012 Investigation; and

e. the extent of the overall information deficit, for both users and non-users, and its negative impact on the fairness of the processing carried out by WhatsApp.

WhatsApp's Submissions and Assessment of Decision-Maker

819. WhatsApp has submitted[442] that "*nowhere in the Supplemental Draft does the Commission explain how its assessment in relation to each of the Article 83(2) [criteria] has informed the level of the proposed administrative fines*."

820. It has further submitted, in this regard, that:

> *"there is no discernible link apparent in the Supplemental Draft between the Commission's consideration of the Article 83(2) [criteria] and the subsequent determination of the level of the proposed administrative fines. While the Commission sets out various considerations in relation to the Article 83(2) [criteria], it does not explain how such considerations have influenced the proposed ranges of the administrative fines. Consequently, WhatsApp lacks insight into the Commission's weighting of these factors in determining the proposed fines and this makes it difficult for WhatsApp to meaningfully respond to the Commission's determinations on quantum[443]."*

821. I note that the GDPR is silent, as regards the particular process or methodology which the Commission should adopt in calculating any fine. As a matter of EU law, however, the Commission must take a decision which allows the addressee to understand the basis for the fine and the effect of the Article 83(2) criteria[444]. As a matter of Irish domestic law, the Commission's decision must be demonstrably rational and not arbitrary. This requires the Commission to be able to explain how it arrived at the level of the fine. In these circumstances, and in view of the lack of direct GDPR guidance, it is relevant to examine the approach (where properly analogous) in EU competition law. This is the area of EU law where fines are most commonly applied; Recital 150 of the GDPR further expressly invokes Articles 101 and 102 TFEU, at least for the purpose of defining an undertaking.

822. Considering the position by reference to EU competition law fining regimes where the Competition Fining Guidelines do not apply (a situation which is similar to the present situation whereby no specific guidance on the calculation of GDPR fines is available), I note that the General Court has established[445] that:

> *"Where the [European] Commission has not adopted any guidelines setting out the method of calculation which it is required to follow when setting fines under a particular provision and the Commission's reasoning is disclosed in a clear and unequivocal fashion in the contested decision, the Commission is not required to express in figures, in absolute terms or as a percentage, the basic amount of the fine and any aggravating or mitigating circumstances."*

823. In terms of the fines proposed above, I am satisfied that I have set out the supporting reasoning in clear and unequivocal terms, by reference to my analysis of the Article 83(2) criteria. In terms of the figures selected, I note that the maximum fines permitted to be imposed pursuant to the GDPR are set at a very high level. This clearly indicates that the GDPR contemplates robust and significant penalties in appropriate cases. The fines proposed above reflect the nature and gravity of the Infringements and satisfy the requirement, pursuant to Article 83(1), for fines to be "effective,

[442] The Supplemental Draft Submissions, paragraph 16.3
[443] The Supplemental Draft Submissions, paragraph 4.2
[444] See, by analogy, HSBC Holdings plc and Others v Commission, T-105/17, ECLI:EU:T:2019:675, paragraphs 336 -354
[445] Marine Harvest ASA v European Commission, Case T-704/14, ECLI:EU:T:2017:753, judgment of General Court dated 26 October 2017, paragraph 455

proportionate and dissuasive". I am further satisfied that the fine is no greater than required to achieve deterrent effect, noting the industry in which WhatsApp operates, the extent of internal and external resources available to it, WhatsApp's submissions, as regards its parity of approach to transparency with its industry peers and the instructions of the Board in its Article 65 Decision.

824. WhatsApp further submits that "*the Commission's attempt to draw any parallel between the current Inquiry and the CNIL's investigation into Google LLC is misplaced and inappropriate*." I do not agree that this is the case. I have considered WhatsApp's submissions, as regards why it believes the Google case to be distinguishable from the within Inquiry. I am satisfied, however, that it is appropriate for me to consider the fines that I have decided to impose as against those imposed in the Google case. I wish to take the opportunity to, again, emphasise that I have noted the CNIL Decision for the purposes of the consistency principle only. I have not based my decision on it. To be absolutely clear about the position, the within decision is my own and is based on the evidence and submissions which I have considered and my assessment of same within the context of the legal framework of the GDPR as well as the instructions of the Board, further to its Article 65 Decision. Further, while I note WhatsApp's submission that I should give due regard to a wider range of decisions for this purpose, WhatsApp will appreciate that the range of suitably analogous decisions is somewhat limited given that the GDPR fining regime has only been in effect since 25 May 2018.

825. For the avoidance of doubt, I do not agree that the circumstances of the two decisions which have been specifically cited by WhatsApp are suitably analogous to the circumstances of the within Inquiry. In relation to the CNIL's Decision[446] concerning SPARTOO SAS, I note that the data controller concerned did not operate in every EU Member State; rather it operated sixteen websites within thirteen EU Member States. Further, the findings of infringement found by the CNIL affected a significantly smaller pool of data subjects; the decision records that the data controller concerned had over 11 million customer accounts, over 30 million prospects (which I understand to mean prospective customers) and approximately 1,000 employees. This is in direct contrast to WhatsApp, which, as set out above, is the data controller for approximately 326 million data subjects in the EEA (including the UK). This does not include the pool of affected non-users, which I have estimated to be in the region of 125 million people.

826. In terms of the infringements found, the infringements concerned the breach of Articles 5(1)(c), 5(1)(e), 13 and 32 of the GDPR, arising from the processing of excessive customer data, the excessive retention of customer/prospective customer data, the recording of calls between customers and employees and the absence of security as regards passwords providing access to customer accounts. In terms of the transparency aspect of infringement, the decision reflected the failure by the data controller to comply with certain discrete obligations, namely to notify data subjects of certain transfers of personal data outside of the EU, failure to identify the appropriate legal basis and inadequate provision of information to employees concerning the recording of their data. In contrast, the Infringements found in this Decision reflect a significant level of non-compliance in relation to transparency. As already observed, transparency is one of the core (Article 5) principles that underpin the fair processing of personal data and, accordingly, the Infringements impact on all of the processing carried out by WhatsApp. In other words, the Infringements are not limited to certain categories of data subjects or certain types of processing.

[446] Deliberation of the Restricted Committee SAN-2020-003 of 28 July 2020 relating to SPARTOO SAS

827. In terms of the extent of data undergoing processing, while I note the CNIL's concerns about the sensitivities associated with financial ("bank") data, the range of personal data undergoing processing, while greater than the within case, is not such that it might be said to be a significantly distinguishing factor. Further, the decision records that the CNIL took into account the measures which the company implemented during the sanction proceedings to ensure partial compliance. As already observed, while WhatsApp has been proactive in voluntarily amending its privacy policies, it has only just begun (as of December 2020) to implement those changes (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes). In the circumstances, I am satisfied that this is not a suitably analogous decision, for consistency purposes. I further note that, in addition to the imposition of an administrative fine, the CNIL further imposed an order to bring processing operations into compliance along with an additional sanction of publication for a period of two years.

828. As regards the decisions made by the Commission[447] concerning Tusla (the Irish Child and Family Agency), referenced in a footnote[448] to the Supplemental Draft Submissions, WhatsApp correctly notes that the circumstances of these decisions are "quite different" to the within inquiry. This, in my view, is an understatement of the position, in that the circumstances of the decisions concerned are completely different, in every respect, to the circumstances of the within inquiry. While the nature of those breaches (which, in each case, was symptomatic of an infringement of Article 32(1), and, in some cases, resulted in an infringement of Article 33(1)) was severe, the number of data subjects affected, in each case, was limited to a small number of data subjects. Further, the infringements of Article 32(1) affected specific aspects of the data controller's operations. This is in stark contrast to the circumstances of the within inquiry. While WhatsApp has observed that the fines imposed[449] "appear extremely low", it is important to note that the 2018 Act imposes a limit of €1,000,000, in terms of the maximum fine that may be imposed on a public body that does not act as an undertaking. Further, the Commission considered that the level of the fine was sufficient to ensure that it was "effective, proportionate and dissuasive" to the circumstances, noting, in this regard, the limited budget of the organisation in question. The imposition of a higher fine, in the circumstances, would not have achieved any greater deterrent effect.

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

Assessment of any factors requiring the adjustment of the proposed fines

<u>The Article 83(3) Limitation</u>

830. Turning, firstly, to Article 83(3), I note that this 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."*

[447] Available at: https://dataprotection.ie/en/dpc-guidance/law/decisions-made-under-data-protection-act-2018
[448] The Supplemental Draft Submissions, footnote 92 (as referenced in paragraph 17.2(B))
[449] Noting that, as at the date hereof (23 December 2020), only the first (in time) of the fines imposed has been confirmed by the Irish Courts, as required by Section 143 of the 2018 Act.

831. As set out above, the Infringements concern simultaneous negligent breaches of Articles 5, 12, 13 and 14 in the context of the same set of processing operations. Accordingly, and by reference to Article 83(3), I expressed the view, in the Composite Draft, that the amount of any consequent fine(s) cannot exceed the amount specified for the gravest infringement. When preparing the Composite Draft, I considered the infringement of Article 14 in the context of non-users to be the most serious of the (then three) infringements. On this basis, I proposed to limit the fine to be imposed to the amount corresponding to the Article 14 infringement.

WhatsApp's Response and Assessment of Decision-Maker

832. While WhatsApp agrees with the identified manner of operation of Article 83(3), it disagreed[450] with the proposed finding that the Article 14 Infringement is the most serious of the three Infringements. I have already considered the reasons put forward in support of this particular submission, as part of my assessments of (i) the Submissions on Recurring Themes, and (ii) the Article 83(2) criteria.

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

833. The German (Federal), French and Portuguese SAs each raised an objection to the manner in which I proposed to interpret and apply Article 83(3). The objections collectively identified various concerns that the approach proposed would "limit the possible maximum amount of the total fine in a disproportionate way", hamper the "imposition of dissuasive fines" or "largely amputate" the high level of sanctions provided for by the GDPR[451]. In the view of the CSAs, the word 'specified', in Article 83(3), refers to the fining cap for the most serious frame abstractly provided for in the GDPR, in a case where infringements of several provisions of the GDPR are found to have occurred; in other words, the purpose of Article 83(3) is to assist with the identification of the applicable fining cap in any case where multiple infringements of the GDPR are under assessment.

834. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, this matter was included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objections, the Board determined[452] as follows:

> *315. "All CSAs argued in their respective objections that not taking into account infringements other than the "gravest infringement" is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found[453] and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case [454]. 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 [455].*

[450] The Supplemental Draft Submissions, paragraphs 18.1 – 18.4, inclusive
[451] The Article 65 Decision, paragraph 304
[452] The Article 65 Decision, paragraphs 315 to 327, inclusive
[453] IE SA Composite Response, paragraph 72(b)(i).
[454] IE SA Composite Response, paragraph 72(b)(iv).
[455] Draft Decision, paragraph 774.

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 [456], 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 [457]. 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 [458]. 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 [459].

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

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

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

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

322. As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the effet utile principle requires all institutions to give full force and effect to EU law [460]. 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

[456] Draft Decision, paragraph 747.
[457] WhatsApp Article 65 Submissions, paragraph 35.1.
[458] WhatsApp Article 65 Submissions, paragraph 35.3.
[459] WhatsApp Article 65 Submissions, paragraph 35.6-35.12.
[460] See, *inter alia,* Antonio Muñoz y Cia SA, e.a. v. Frumar Ltd e.a. (Case C-253/00, judgment delivered 17 September 2002) ECLI:EU:C:2002:497, paragraph 28 and the case law cited.

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 [461] 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" [462]. 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."

835. Pursuant to Article 65(6), I am bound to adopt both the binding determination and associated rationale of the Board. This Decision is hereby amended to reflect a position whereby Article 83(3) does not provide for concurrency in fining, but, rather, identifies only the applicable fining cap. Pursuant to the Board findings, this Decision records findings of infringement of Articles 5, 12, 13 and

[461] Article 29 Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679' (3 October 2017), WP 253, endorsed by the EDPB on 25 May 2018, hereinafter "Guidelines on Administrative Fines".
[462] Guidelines on Administrative Fines, p. 10.

14. Each of those provisions are encompassed by Article 83(5) and, accordingly, the "total amount" of the applicable fine shall not exceed the amount specified by Article 83(5).

WhatsApp's response to the assessments recorded above and the response of the Decision-Maker

836. By way of submissions dated 19 August 2021 ("the **Final Submissions**"), WhatsApp exercised its right to be heard in response to the Commission's proposals arising from the Board's instruction, requiring it to reassess and increase the fine previously proposed by the Composite Draft, taking into account the matters set out in Section 9.4 of the Article 65 Decision. To that end, WhatsApp was provided with a copy of the relevant part of the working draft of the Commission's amended decision (i.e. a version of the Composite Draft that was in the process of being amended, for the purpose of compliance with Article 65(6), to take account of the determinations made by the Board in its Article 65 Decision) ("the **Extract**").

837. The Final Submissions sought to challenge the manner and outcome of the Commission's reassessment of the fine under five headings, as follows[463]:

Heading 1: Failure to adequately address the Article 83(2) factors in respect of the fines proposed, with particular reference to the Article 5(1)(a) infringement

838. Under this heading, WhatsApp submitted[464] that:

a. The Extract does not adequately address the Article 83(2) factors in respect of each infringement and instead assesses and applies these factors "generically and collectively".

b. There is no clear (or any discernible) link between the Commission's consideration of the Article 83(2) factors and the subsequent determination on the level of the proposed fine for the Article 5(1)(a) infringement (or any of the other infringements). The Commission has cumulatively assessed the infringements but proposes to impose separate fines. Such an approach does not satisfy the requirement for legal certainty.

c. There is no justification for the proposed fines. By way of example:

i. In terms of the **nature** of the Article 5(1)(a) infringement, the Commission appears to rely on matters beyond the finding of infringement itself by reference to the statement that the failure to comply with the transparency principle potentially undermines "*other fundamental data protection principles, including but not limited to the principles of fairness and accountability*." WhatsApp submits, in this regard, that the Board did not direct the Commission to include a finding of infringement of the accountability principle. WhatsApp further submits that it fails to see how the Commission can seek to rely on "potential" undermining of other principles (which WhatsApp has not been found to have infringed) to support the proposed fine.

[463] The Final Submissions, paragraph 2.1
[464] The Final Submissions, paragraphs 3.1 to 3.3

ii. In terms of the **gravity** of the Article 5(1)(a) infringement, the Commission has failed to have regard to the overlapping nature of the infringements. The Commission, in this regard, must identify the gravity that is attributable to the Article 5(1)(a) infringement alone. Given the significant "and arguably complete" overlap between the infringements of Article 5 and Articles 12 to 14, the Commission cannot attach much, if any, weight to this factor in determining the fining amount.

iii. The Extract states that the infringements "remain ongoing". The Commission, however, should take account of the updates made to the Privacy Policy in January 2021, as a mitigating factor.

iv. The Commission is not entitled to take a factor that has been deemed to be an aggravating factor in the context of the Article 12 – 14 infringements into account again as a significant aggravating factor for the purpose of imposing a fine for the Article 5(1)(a) infringement.

v. The Commission ought to take account, as a mitigating factor, of the lack of relevant previous infringements and the degree of effort on WhatsApp's part to avoid damage and to cooperate with the Commission.

839. In response to the above, I note that the core theme running throughout WhatsApp's Final Submissions is the overlap between the infringement of Article 5(1)(a) and the infringements of Article 12 – 14. In that regard, there is no doubt but that there is overlap between the Articles 12 – 14 infringements and the Article 5(1)(a) infringement. That is the consequence of the rationale[465] upon which the Board determined the existence of the Article 5(1)(a) infringement. The Commission notes, in this regard, the Board's view that "*an infringement of the transparency obligations under Articles 12 – 14 GDPR can, depending on the circumstances of the case, amount to an infringement of the overarching principle of transparency under Article 5(1)(a)*." In having considered the circumstances of the within inquiry, the Board determined that this was a case in which an infringement of the transparency obligations under Article 12 – 14 amounted to an infringement of the overarching principle of transparency under Article 5(1)(a). The Board noted that this was the case due to the "*gravity and the overarching nature and impact of the [Article 12 – 14] infringements, which have a significant negative impact on all of the processing carried out by [WhatsApp]*."

840. Notwithstanding the above, I disagree with WhatsApp's submission that the Extract does not adequately address the Article 83(2) factors in respect of each infringement. Given the rationale for the Board's determination above, it stands to reason that there will be overlap, in terms of the assessment of the individual infringements for the purpose of Article 83(2). That does not mean, however, that each infringement has not been individually assessed. That ought to be clear from the references to the individual infringements, within the assessments of the Article 83(2) criteria, noting any particular issues arising in any case. I therefore further disagree with WhatsApp's submission that the Commission has cumulatively assessed the infringements but proposes separate fines. This is clearly not the case, as should be evident from the narrative set out in paragraphs 697 and 698, above.

[465] See the Article 65 Decision, paragraphs 193 to199

841. In terms of the justification for the proposed fines, WhatsApp has suggested that I am not entitled to have regard to the potential negative impact of infringement of the transparency obligations on other fundamental data protection principles. Such a submission is inconsistent with the view expressed[466] by the Board, in the Article 65 Decision, that "*transparency … is intrinsically linked to the principle of accountability under the GDPR*". The Board further underlined that "*the principle of transparency is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive*." Accordingly, and in circumstances where Board has recognised the interconnection and interdependence between the transparency obligation and other fundamental data protection principles, it is not only appropriate but necessary for me to have regard to such matters when carrying out the Article 83(2) assessment for the purpose of the Article 5(1)(a) infringement.

842. I note that I have already set out my views, as part of my assessment of the Submissions on Recurring Themes, on the weight that I might attribute to WhatsApp's having made amendments to its Privacy Policy on a voluntary basis. The views so expressed apply equally here. As regards WhatsApp's submission concerning the "ongoing" nature of the infringements, it is important to note that the assessment of duration (as with all of the Article 83(2) assessments recorded in this Decision) is that which was set out in the Composite Draft that entered the Article 60 co-decision-making process in December 2020. That being the case, the assessment of duration, for the purpose of the Article 5(1)(a) infringement covers the same period (i.e. to December 2020) in circumstances where the Board determined the existence of the Article 5(1)(a) infringement by reference to the existing findings of infringement of Articles 12 – 14. I further note that the Board, having considered the manner in which the Commission assessed duration, as recorded in the Composite Draft, determined that "*the [draft decision] does not need to be amended regarding consideration of the duration as an aggravating factor*". As noted elsewhere in this Decision, the Commission is bound by the findings and determinations recorded in the Article 65 Decision.

843. I note that I have already set out my views, as part of my assessment of the Submissions on Recurring Themes, on the weight that may be attributed, as a mitigating factor, to the lack of relevant previous infringements, WhatsApp's good faith efforts and its cooperation with the Commission. The views so expressed apply equally here.

Heading 2: Non-compliance with the requirements of Article 83(1), resulting in a situation whereby the reassessed fines are "disproportionate, excessive and unnecessary"

844. WhatsApp has submitted[467], in this regard, that:

a. the proposed fines far exceed what is required by Article 83(1) and that this applies in particular to the fine that has been proposed in respect of the Article 5(1)(a) infringement.

b. The Commission has failed to meaningfully engage with Article 83(1) and there appears to be a failure to adequately consider whether, taken as a whole, the total of the proposed fines in respect of all of the infringements are effective, proportionate and dissuasive.

[466] The Article 65 Decision, paragraph 188
[467] See the Final Submissions, paragraphs 4.1 to 4.7

c. The Commission was previously satisfied that the overall fine it proposed (of €30 to €50 million) was sufficient to be effective in light of all of the circumstances of the inquiry. This demonstrates the extent to which the Extract fails to have regard to the requirements of Article 83(1).

d. As before, inadequate account has been taken of the nature of the infringements, the good faith efforts taken by WhatsApp to comply prior to and during the inquiry and the lack of any demonstrable harm to data subjects.

845. In response to the above, it is important to remember that this Decision is being made within a consensus-based, co-decision-making process. In these circumstances, it is irrelevant that the Commission previously considered the fine proposed by the Composite Draft to be effective, proportionate and dissuasive in light of the circumstances of the within inquiry. I further note, in this regard, that I advised WhatsApp, by way of letter dated 23 April 2021 that, when selecting the final fine (i.e. when exercising the discretionary element within the fining process) that I would take account of both WhatsApp's views as well as the views of the CSAs.

846. Against the background of the above, it is important to reflect on the expectations that have been expressed by a range of CSAs within the co-decision-making process to date. As WhatsApp is aware, a number of CSAs have indicated their view that the fine to be imposed ought, more appropriately, to be closer to the maximum fining range of 4% of the turnover of the undertaking concerned (which, in this case, has been established, by the Board, to be the Facebook, Inc. family of companies).

847. It is further important to note that the Commission is subject to a binding decision of the Board that requires an upwards[468] reassessment of the fine originally proposed by the Composite Draft, taking into account the various determinations of the Board that are recorded in Section 9.4 of the Article 65 Decision. Those matters include the requirement for the Commission to take account of the turnover of the undertaking concerned when calculating the fine, as well as each of the findings of infringement (including the new and extended findings that were established by the Board elsewhere in its Article 65 Decision) that were found to have occurred in this inquiry. Section 9.4 of the Article 65 Decision comprises six different matters in total. In the circumstances, it is difficult to understand how the required reassessment might not have resulted in a substantial increase in the fine originally proposed by the Composite Draft.

848. Further, I disagree that the Commission has failed to take any, or adequate, account of Article 83(1) when assessing whether the total amount of the fines proposed was effective, proportionate and dissuasive in the circumstances of the case. The Commission has followed the determination made by the Board, in the Article 65 Decision, arising from its assessment of those CSA objections that expressed the view that the fine originally proposed by the Composite Draft was not effective, proportionate and dissuasive, for the purpose of Article 83(1). The Board has clearly rationalised its determination (as set out at paragraph 807, below) and the Commission has adhered to the guidance provided.

[468] The Article 65 Decision, paragraph 424

849. As before, I have already considered, as part of my assessment of the Submissions on Recurring Themes, WhatsApp's submissions concerning the account that ought to be taken of the specified (mitigating) factors.

Heading 3: Incorrect implementation of Article 83(3), "even taking into account the [Article 65 Decision]"

850. WhatsApp has submitted[469], under this heading, that:

a. The Board's interpretation does not mandate the approach the Commission proposes to take in the Extract of setting a fine for each infringement in isolation, without assessment of overlap, and then adding these up to produce a cumulative fine without regard to Article 83(1).

b. Neither the GDPR nor the Board prescribes the Commission's proposed approach. The Article 65 Decision leaves room for the Commission to respect the overlapping nature of the infringements in order to establish what would be an effective, proportionate and dissuasive total.

c. Proposing a new fine in respect of the Article 5(1)(a) infringement and then simply adding it together with the other fines leads to (at least) a double penalty being imposed for the same matters under assessment.

851. I note that the submissions made under this heading overlap somewhat with the previous headings. I have already addressed the overlapping nature of the infringements in my response to the submissions made under Heading 1. I have further addressed WhatsApp's Article 83(1) submissions as part of my response to the submissions made under Heading 2.

852. As regards the submission concerning double punishment (including the application of the principle of ne bis in idem), it is firstly important to remember that the Commission is subject to binding determinations of the Board, requiring the Commission to amend the Composite Draft to (i) record a finding of infringement of Article 5(1)(a); and (ii) reassess the proposed fine to take account of the matters identified in Section 9.4 of the Article 65 Decision, including the requirement for the Commission to "take into account the other infringements – in addition to the gravest infringement[470]". The Commission further notes, in relation to the Board's determination that an infringement of Article 5(1)(a) has occurred in this case, that the Article 65 Decision records WhatsApp's submission[471] that "the controller cannot be punished twice for the same conduct" and WhatsApp's reliance on the statement made by the CNIL whereby it indicated that it could not see "on which facts, not already covered by the breach to (sic) article 12, the breach to (sic) article 5(1)(a) would be based" and its further comment whereby it wondered "if [the addition of fines in respect of such additional infringements] would be compatible with the principle according to which the same facts should be punished only one time". While the Article 65 Decision does not record the manner in which the Board took account of WhatsApp's submissions, it is clear, by reference to the determinations that it ultimately made (requiring the Commission to record a finding of infringement of Article 5(1)(a) and to take that finding into account when making an upward reassessment of the

[469] See the Final Submissions, paragraphs 5.1 to 5.9
[470] The Article 65 Decision, paragraphs 327, 423, 430 (second bullet point),
[471] The Article 65 Decision, paragraph 186

proposed fine), that it did not agree with WhatsApp's submissions concerning double punishment for the same conduct. I further note that the only way to avoid this risk would be for the Commission to not take account of (or "reflect[472]") either the Article 5(1)(a) infringement or the Article 12 – 14 infringements when reassessing the proposed fine. This course of action, however, is not open to the Commission, in circumstances where it is subject to a binding decision of the Board that requires it to carry out an upwards reassessment of the fine originally proposed to take account of six factors, including the requirement for the Commission to take account of each of the existing and new/extended findings of infringement in that fine.

Heading 4: Incompatibility with EU law principles and the specific nature of the concurrence of Articles 5 and 12 to 14

853. WhatsApp has submitted[473], under this heading, that:

a. The manner in which the fines have been calculated offends against the EU law principle of "ne bis in idem" and concurrence of laws. This means that, in a case of multiple offences caused by a single conduct, the competent authority or court can only impose one single sanction limited by the gravest offence – or at a minimum in the present context one sanction limited by the combined gravity of the offences accurately addressed *in the round*.

b. The fine being proposed for the Article 5(1)(a) infringement by itself has the effect of almost doubling the fines to be imposed for what is essentially the same set of facts and alleged infringement. The sanctions already proposed for the infringements of Articles 12 to 14 already take due (and in fact, when combined, excessive) account of the seriousness of the transparency infringement.

854. Again, there is a significant degree of overlap between the submissions made under this heading and those made under the previous headings. In response to the new elements, it is important to note, from the figures set out in Articles 83(4) – (6), that the legislator envisaged a robust fining regime to address infringements of the GDPR. This is clear not only from the static maximum fining caps set out in Articles 83(4) – (6) but also the inclusion of dynamic maximum fining caps, applicable to undertakings (which, as clarified by Recital 150, has the same meaning as in EU competition law). In these circumstances, I do not agree that the fines proposed by the Extract are excessive.

855. As regards the application of the principle of "ne bis in idem", I note that I have already addressed this above, in my response to the submissions made under Heading 3.

Heading 5: The fine proposed for the Article 14 infringement ought to be significantly reduced

856. WhatsApp has submitted[474], under this heading, that:

a. As before, WhatsApp has sought to rely on the fine originally proposed by the Composite Draft in support of its assertion that the Commission was previously satisfied that the fine

[472] The Article 65 Decision, paragraph 423
[473] See the Final Submissions, paragraphs 6.1 to 6.8
[474] See the Final Submissions, paragraphs 7.1 to 7.5

proposed for the Article 14 infringement (in the range of between €30 and €50 million) was effective, proportionate and dissuasive in the circumstances of the inquiry, "taking into account all infringements."

b. WhatsApp has further submitted that, rather than reassessing the fine originally proposed in respect of the Article 14 infringement, the Commission has simply reverted to the fine previously proposed without having any regard to WhatsApp's previous submissions, made in response to the fine originally proposed.

857. In response to the above, WhatsApp appears to be suggesting that the fine proposed by the Composite Draft reflected all of the (then) three infringements that were found to have occurred. To be absolutely clear about the position, this is absolutely not the case and it is difficult to understand how WhatsApp could have formed this view, given the clear explanation, set out in the Composite Draft, as to the manner in which the Commission interpreted and applied Article 83(3).

858. As regards the Commission's reinstatement of the fine originally proposed by the Supplemental Draft in respect of the Article 14 infringement, the manner in which the Commission has taken account of WhatsApp's various submissions is clearly set out in Part 5 of this Decision, including within the individual Article 83(2) assessments as well as my assessments of the Submissions on Recurring Themes. It is therefore incorrect to suggest that the Commission failed to have regard to WhatsApp's submissions. I further question why it might have been inappropriate for the Commission to have reinstated the fine that it originally proposed in circumstances where the impact, from the perspective of the Article 83(2) assessment, of the Board's determination on the lossy hashing objections is materially identical to that originally outlined in the Preliminary Draft and Supplemental Draft decisions.

859. On the basis of the above, I am not inclined to make a downward adjustment to the fines proposed above to take account of WhatsApp's Final Submissions.

Article 83(5) and the applicable fining "cap"

860. Turning, finally, to Article 83(5), I note that this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement, 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:*
> *…*
> *(b) the data subjects' rights pursuant to Articles 12 to 22;*
> *…"*

861. 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."*

862. 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, that the Court of Justice of the EU ("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*[475]"

863. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement[476].

864. In the context of Article 83, the concept of 'undertaking' means that, where there is another entity, such as a parent company, 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.

865. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case[477].

866. The CJEU has, however, established[478] that, where a parent company has a 100% shareholding in a subsidiary, it follows that:

    a. the parent company is able to exercise decisive influence over the conduct of the subsidiary; and

    b. a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

867. 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

[475] *Höfner and Elser v Macrotron GmbH* (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161 §21
[476] *Akzo Nobel and Others v Commission*, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, § 58 - 61
[477] Ori Martin and SLM v Commission (C-490/15 P, judgment delivered 14 September 2016) ECLI:EU:C:2016:678 § 60
[478] Akzo Nobel and Others v Commission, (C-97/08 P, judgment delivered 10 September 2009)

over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary[479].

868. 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 a decisive influence over the conduct of its subsidiary[480]. This reflects the position that:

> "*… the presumption of actual exercise of decisive influence is based, in essence, on the premiss 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 …*[481]"

869. 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.

Application of the above to the within inquiry

870. Having reviewed the Directors' Report and Financial Statements filed, on behalf of WhatsApp, with the Irish Companies Registration Office (in respect of the financial period from 6 July 2017 to 31 December 2018)[482], I note that this document confirms, on page 3, that:

> *"Principal activity and review of the business*
>
> *WhatsApp Ireland Limited ("the company") is owned by WhatsApp Inc., a company incorporated in the United States of America, which is its immediate parent undertaking and controlling party. The ultimate holding company and controlling party is Facebook, Inc., a company incorporated in the United States of America.*
>
> *WhatsApp is a simple, reliable and secure messaging application that is used by people and businesses around the world to communicate in a private way. The principal activity of the company is acting as the data controller for European users of the WhatsApp service and the provision of support services to WhatsApp Inc.*
>
> *…*

[479] Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, paragraph 48
[480] 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
[481] 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)
[482] While I note that WhatsApp has since filed its Directors Report and Financial Statements for the financial year ending 31 December 2019, I note that the relevant information set out therein is materially identical to that recorded in this Decision.

Going concern

The company's ultimate parent undertaking, Facebook, Inc., has given written assurances that adequate funds will be made available to the company to ensure that liabilities will be discharged at the amount at which they are stated in the financial statements and to continue to fund the operations of the company for a period of at least twelve months from the date of approval of these financial statements. The company therefore continues to adopt the going concern basis in preparing its financial statements."

871. Page 18 further confirms that:

"Controlling parties

At 31 December 2018, the company was a wholly-owned subsidiary of WhatsApp Inc., a company incorporated in Wilmington, Delaware, United States of America.

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."

872. On the basis of the above, it appears that:

a. WhatsApp is the wholly owned subsidiary of WhatsApp Inc.;

b. WhatsApp Inc. is ultimately owned and controlled by Facebook, Inc.; and

c. As regards any intermediary companies in the corporate chain, between WhatsApp and Facebook, Inc., it is assumed by reference to the statement recorded above, that the "*ultimate holding company and controlling party of the smallest and largest group of which [WhatsApp] is a member … is Facebook, Inc.*"

873. It follows, therefore, that:

a. The corporate structure of the entities concerned and, in particular, the fact that Facebook, Inc. owns and controls WhatsApp Inc. means that Facebook, Inc. is able to exercise decisive influence over WhatsApp's behaviour on the market; and

b. A rebuttable presumption arises that Facebook, Inc. does in fact exercise a decisive influence over the conduct of WhatsApp on the market.

874. If this presumption is not rebutted, it means that Facebook, Inc. and WhatsApp constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU.

875. Having put[483] the above to WhatsApp, WhatsApp confirmed[484] that:

[483] By way of letter dated 24 April 2020 from the Commission to WhatsApp
[484] By way of letter dated 1 May 2020 from WhatsApp to the Commission

a. "[It] is a wholly-owned subsidiary of WhatsApp Inc.; and

b. WhatsApp Inc. is ultimately a wholly-owned subsidiary of Facebook, Inc."

876. WhatsApp, however, did not furnish any evidence directed to the rebuttal of the presumption. Instead, it advised that:

"To the extent relevant (if at all) to the imposition or amount of any administrative fine under the GDPR (please see the questions we have in this respect below), we do not believe that, as a result of the corporate structure of the entities concerned, either WhatsApp Inc. or Facebook, Inc. exercises "decisive influence" over [WhatsApp's] "behaviour on the market" in the way that such phrases would need to be interpreted in order to make sense in the context of the GDPR."

877. In response to my request[485] that WhatsApp bring the matter to the attention of "any parent or controlling company as might be required to fully address the matters raised" WhatsApp advised[486] that:

"While neither WhatsApp Inc. nor Facebook, Inc. are parties to the Inquiry, we confirm that we have brought your letter and this response to the attention of personnel at WhatsApp Inc. and Facebook, Inc. on a voluntary basis. However, it is not clear at present how input from those entities might be required to address the matters raised in your letter, or why they might have matters to raise which could be relevant in the circumstances. We would be grateful for any clarification you are able to provide in this respect, and we can then consider the matter further."

878. I wrote further to WhatsApp[487], answering each of the questions raised and providing the clarification sought. I repeated the presumption arising and repeated my request that WhatsApp confirm whether or not it agreed with my assessment. As before, I requested that, in the event that WhatsApp did not agree with my assessment, it should detail "by reference to the economic, organisational and legal links between the [entities concerned], why [it so disagreed]". I also repeated my request that WhatsApp bring my letter to the attention of "any parent or controlling company, as might be required to fully address the matters raised".

879. In response[488], WhatsApp (via its legal advisors) advised that it did not agree with the position that had been outlined in relation to how "competition law concepts" should be transposed to the "very different statutory context of the GDPR". WhatsApp advised that it had not set out "the detailed reasons why it disagrees" with the position that had been outlined to it and that:

"Instead, [WhatsApp] reserves its right to raise these reasons at the appropriate stage in the Inquiry, namely in response to any draft corrective measures decision, if necessary."

880. Notwithstanding the reasons subsequently raised by WhatsApp in its response to the Supplemental Draft (which I have dealt with below), by reference to the information set out above and in the absence of any evidence to the contrary, I find that:

[485] Included in the letter dated 24 April 2020 from the Commission to WhatsApp
[486] Included in the letter dated 1 May 2020 from WhatsApp to the Commission
[487] By way of letter dated 18 May 2020, from the Commission to WhatsApp
[488] Communicated by way of letter dated 25 May 2018 from Mason Hayes & Curran, solicitors to the Commission

a. The corporate structure of the entities concerned and, in particular, the facts that:

i. WhatsApp is a wholly-owned subsidiary of WhatsApp Inc.; and

ii. WhatsApp Inc. is a wholly-owned subsidiary of Facebook, Inc.

means that Facebook, Inc. is able to exercise decisive influence over WhatsApp's behaviour on the market;

b. On this basis, a rebuttable presumption arises that Facebook, Inc. does in fact exercise a decisive influence over the conduct of WhatsApp on the market;

c. This presumption has not been rebutted; and

d. Consequently, WhatsApp and Facebook, Inc. constitute a single economic unit and, thereby, a single undertaking for the purpose of Articles 101 and 102 TFEU.

881. Applying the above to Article 83(5), I firstly noted that, in circumstances where the fine is being imposed on an 'undertaking', a fine of up to 4% of the total worldwide annual turnover of the preceding financial year may be imposed. WhatsApp confirmed[489] that the combined turnover for Facebook, Inc. and WhatsApp Ireland for the year ending 31 December 2019 was approximately [redacted]. That being the case, the fine proposed to be imposed (in respect of the Article 14 Infringement), did not exceed the applicable fining "cap" prescribed by Article 83(5).

WhatsApp's Submissions and Assessment of Decision-Maker

882. As noted above, WhatsApp raised objections on the rationale set out above, which had been set out in the Supplemental Draft. In doing so, WhatsApp submitted[490] that the views set out above, as to the manner of identification of the relevant undertaking are "*wrong as a matter of fact and law*". While reserving its right to make submissions "*in relation to such matters in due course as necessary or appropriate*", WhatsApp summarized the reasons why it disagrees with the Commission's assessment, as follows:

a. The competition law concept of decisive influence does not directly translate in the context of the GDPR, which pursues different objectives to Articles 101 and 102 TFEU.

b. The Commission has not engaged with the question as to what "behavior on the market" means in a GDPR context.

c. "*For the competition law concept of decisive influence to have any real meaning in the context of the GDPR, it must be adapted accordingly, in a similar way to how the concept of "dominant influence" in Recital 37 GDPR has been adapted … by encompassing, for example, the ability to control the processing activities of subsidiaries*".

[489] By way of its letter to the Commission dated 1 October 2020
[490] The Supplemental Draft Submissions, paragraphs 18.5 to 18.9 (inclusive)

d. Accordingly, in order to determine whether Facebook, Inc. exercises decisive influence over WhatsApp's "conduct on the market" for the purposes of the GDPR, the Commission's analysis should properly focus on WhatsApp's data processing activities and the related decision-making about personal data processed by WhatsApp.

e. On the basis of the above, Facebook, Inc. cannot properly be said to have "decisive influence" when that term is considered in a GDPR context.

883. I note that I have already addressed, at length, the substance of the above submissions by way of a letter dated 18 May 2020 to WhatsApp. I do not propose to traverse the same ground here, given that WhatsApp is already aware of my position on the matters raised. My position, therefore, remains that, for the reasons set out above, WhatsApp and Facebook, Inc. constitute a single economic unit and, thereby, a single undertaking for the purposes of Article 101 and 102 TFEU and, indeed, for the purposes of Article 83(5) of the GDPR.

884. As noted above, the concept of "turnover" is also critical to the provisions of Article 83(5), in relation to the imposition of an administrative fine. Arising from matters which were referred to the Board pursuant to the Article 65 dispute resolution process, as described below, in relation to the concept of "turnover", I have incorporated the binding determination and rationale of the Board on these matters, as set out below, into this Decision, in order to identify the relevant turnover of the relevant undertaking for the purposes of Article 83(5) and the calculation of the fine.

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

885. The German (Federal) SA raised objections to the Commission's analysis of the applicable turnover figure on the basis that:

b. The overall turnover of the single economic unit should be used in the context of Article 83, instead of the combined turnover of Facebook, Inc. and WhatsApp; and

c. The turnover figure to be used should be that of the financial year immediately preceding the date of the relevant decision (rather than the last complete financial year immediately preceding the circulation of the draft decision for the purpose of Article 60).

886. As it was not possible to reach consensus on all of the issues raised at the Article 60 stage of the co-decision-making process, the matter was included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objections, the Board determined[491] as follows:

"<u>Determination of the relevant turnover of the undertaking</u>

286. The DE SA raised an objection stating that as Facebook Inc. and WhatsApp IE were found to be the undertaking by the LSA, the overall turnover of the single economic unit should be used in the context of Article 83 GDPR, instead of the combined turnover of Facebook Inc. and WhatsApp IE only [492]. While the final position taken by

[491] The Article 65 Decision, paragraphs 286 to 292 and 294 to 298 (inclusive)
[492] DE SA Objection, p. 12-13.

the IE SA was to not follow any of the objections [493], in its Composite Response the IE SA expressed its intention to amend this figure to reflect the combined turnover of the entire Facebook, Inc. group of companies [494].

287. The EDPB notes that the IE SA had communicated their assessment of the notion of undertaking to WhatsApp IE, including the application made in the context of Article 83 GDPR. The IE SA requested WhatsApp IE to bring this matter to the attention of "any parent or controlling company as might be required to fully address the matters raised'' [495]. WhatsApp IE confirmed having brought the IE SA's letter and their response to the attention of personnel at WhatsApp Inc. and Facebook, Inc. on a voluntary basis, noting that neither WhatsApp Inc. nor Facebook, Inc. are parties to the Inquiry [496]. WhatsApp IE expressed the view that "the relevant 'undertaking' for the purpose of Articles 83(4) to (6) GDPR is WhatsApp Ireland alone", adding that it "disagrees with the [IE SA]'s approach to the assessment of whether an entity is in a position to exercise 'decisive influence' over WhatsApp Ireland's 'behaviour on the market' in the context of the GDPR" [497]. WhatsApp IE put forward that the interpretation and application of competition law concepts of "undertaking" and "decisive influence" over "conduct on the market" in the very different statutory context of the GDPR raises questions likely to require judicial consideration [498].

288. While the qualification of Facebook Inc. and WhatsApp IE as a single undertaking is not contested by the DE SA, the EDPB notes however that there is a disagreement between the LSA and the CSA on the amount of the turnover to be taken into account for this single economic unit.

289. On this specific issue, and in accordance with Recital 150 GDPR, the EDPB considers the case law of the CJEU in the field of competition law relevant when assessing the turnover to be taken into account in the context of Article 83 GDPR, in particular for the verification of the upper limit of the amount of the fine under Article 83(4)-(6) GDPR.

290. Firstly, according to established case law of the CJEU and as recalled by the IE SA in its Draft Decision [499], when a parent company and its subsidiary are found to form a single undertaking within the meaning of Articles 101 and 102 TFEU, this means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the latter in the infringement. In particular, the parent company may be held liable for the fine [500].

291. Secondly, the CJEU has ruled that when a parent company and its subsidiary form the single undertaking that has been found liable for the infringement committed by the subsidiary, the total turnover of its component companies determines the

[493] See paragraph 13 above.
[494] IE SA Composite Response, paragraphs 63.a.i. and 65.
[495] Draft Decision, paragraphs 793-794.
[496] Letter dated 1 May 2020 from WhatsApp to the IE SA, in response to the letter dated 24 April 2020 from the IE SA to WhatsApp on the concept of undertaking.
[497] WhatsApp Article 65 Submissions, paragraph 31.2.
[498] WhatsApp Supplemental Draft Submission, paragraphs 18.5 to 18.9 (in particular 18.6.D and 18.7).
[499] Draft Decision, paragraph 779.
[500] *Akzo Nobel and Others v. Commission*, (Case C-97/08 P, judgment delivered 10 September 2009), paragraphs 58 - 61.

financial capacity of the single undertaking in question [501]. With regards to the parent company at the head of a group, the CJEU specified that consolidated accounts of the parent company are relevant to determine its turnover [502]. In the present case, this implies the consolidated turnover of the group headed by Facebook Inc. is relevant.

292. In light of the above and bearing in mind that the IE SA qualified Facebook Inc. and WhatsApp IE as a single undertaking in the Draft Decision, the EDPB decides that the IE SA should amend its Draft Decision in order to take into account the total turnover of all the component companies of the single undertaking for the purpose of Article 83 GDPR."

"<u>Preceding financial year</u>

294. The EDPB notes that the IE SA takes into account, for the calculation of the fine, the global annual turnover in the financial year preceding its Draft Decision [503]. In this respect, the DE SA argues that the financial year that should be taken into account is that preceding the final decision of the LSA [504]. Since there is no dispute on the fact that the expression "preceding financial year" refers to the decision of the LSA, the EDPB will therefore focus its assessment on whether such decision shall be the draft or the final one.

295. In the field of competition law, the CJEU has clarified the meaning of "preceding business year" with regards to the power granted to the European Commission to impose fines on undertakings in application of Article 23 of Regulation 1/2003 [505]. As a rule, the maximum amount of the fine "should be calculated on the basis of the turnover in the business year preceding the Commission decision" [506].

296. The IE SA points out that in terms of the one-stop-shop procedure, the "LSA is not a sole decision-maker; rather, it is required to engage with CSAs via the process outlined in Article 60 of the GDPR. That process prescribes consultation periods and a further mechanism for the resolution of disagreements on which consensus cannot be reached. The practical consequence of this is the potential for the significant passage of time between the original circulation of the LSA's draft decision and the adoption of the final decision" [507]. The EDPB concedes the one-stop-shop procedure of Article 60

---

[501] See inter alia *Groupe Gascogne SA v. Commission*, (Case C-58/12 P, judgment delivered 26 November 2013), paragraphs 51-56; Eni v. Commission (C-508/11 P, judgment delivered 8 May 2013), paragraph 109; Siemens Österreich et VA Tech Transmission & Distribution / Commission (T-122/07 à T-124/07, judgment delivered 3 March 2011), paragraphs 186-187.

[502] *Groupe Gascogne SA v Commission*, (Case C-58/12 P, judgment delivered 26 November 2013), paragraphs 52-57.

[503] Draft Decision, paragraph 797.

[504] DE SA Objection, p. 13.

[505] Regulation (EC) No 1/2003 of 16 December 2002 *on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty*. Article 23(1) of Regulation 1/2003 provides that "*The Commission may by decision impose on undertakings and associations of undertakings fines not exceeding 1 % of the total turnover in the preceding business year [...]*".

[506] Laufen Austria AG v. European Commission (Case C-637/13 P, judgement delivered 26 January 2017) ECLI:EU:C:2017:51, paragraph 48; YKK Corporation e.a. v. European Commission (C-408/12 P, judgement delivered 4 September 2014) ECLI:EU:C:2014:2153, paragraph 64. The CJEU has ruled that in certain situations, the turnover of the year preceding the decision of the European Commission to impose fine does not provide any useful indication as to the actual economic situation of the undertaking concerned and the appropriate level of fine to impose on that undertaking. In such a situation, the European Commission is entitled to refer to another business year in order to be able to make a correct assessment of the financial resources of that undertaking and to ensure that the fine has a sufficient and proportionate deterrent effect. See garantovaná a.s. v. European Commission (Case C-90/13, judgement delivered on 15 May 2014) ECLI:EU:C:2014:326, paragraphs 16-17; Britannia Alloys & Chemicals v. European Commission (Case C-76/06 P, judgment delivered on 7 June 2007) ECLI:EU:C:2007:326, paragraph 30.

[507] IE SA Composite Response, paragraph 64.b.i.

GDPR is different from the procedure applicable to the European Commission in the field of competition law. However, in both cases it is true that the fine comes into being only at one point in time, namely when the final decision is issued.

297. At the same time, the LSA is required to circulate a complete draft decision, including where appropriate a fine amount, when it launches the consultation procedure in accordance with Article 60(3) GDPR. The IE SA proposed to maintain in its Draft Decision a reference to the turnover for the financial year ending 31 December 2019, which was the most up to date financial information available to determine the relevant turnover, at the time the draft decision was circulated to the CSAs pursuant to Article 60(3) GDPR. The IE SA further elaborated that "[that] figure will operate as a provisional estimate of the turnover for the financial year ending 31 December 2020. In advance of the final decision, IE SA will obtain from WhatsApp the updated turnover figure for the financial year ending 31 December 2020. That figure will be used to calculate the cap in the final decision. Accordingly, at the time that the final decision is adopted, IE SA will apply the turnover figure for the year ending 31 December 2020 for the purpose of its calculations in Part 4" [508].

298. In light of the above, the EDPB decides that the date of the final decision taken by the LSA pursuant to Article 65(6) GDPR, is the event from which the preceding financial year should be considered. The EDPB 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 [509]."

887. On the basis of the above, including the analysis I have previously undertaken, and on which I have heard from WhatsApp with regard to the concept of undertaking, and adopting both the binding determination and associated rationale of the Board, as required by Article 65(6), in relation to the issue of turnover, this Decision is hereby amended to find that the total worldwide annual turnover of the undertaking concerned[510], for the financial year ending 31 December 2020, is $85.965 billion[511]. As noted above, this is the figure that was taken into account when re-assessing the infringements for the purpose of Article 83(1). This is also the figure that has been used to assess the applicable fining cap. I note, in this regard, that the fine proposed at paragraph 888, below, does not exceed the applicable fining "cap" prescribed by Article 83(5).

Summary of Corrective Powers to be Exercised

888. By way of summary of the outcome of this Decision, I have decided to exercise the following corrective powers:

[508] IE SA Composite Response, paragraph 64.b.iii. The final position of the IE SA was that of not following the objections as clarified above in paragraph 13.
[509] Article 60(6) GDPR, providing that the LSA and CSA are bound by the draft decision on which they (are deemed to) agree, in any case does not apply to the present situation.
[510] The Board concluded, at paragraph 291 of the Article 65 Decision, that "(w)ith regards to the parent company at the head of a group, the CJEU specified that consolidated accounts of the parent company are relevant to determine its turnover. In the present case, this implies the consolidated turnover of the group headed by Facebook Inc. is relevant."
[511] As confirmed by the letter dated 21 July 2021, from WhatsApp's legal representatives to the Commission. See also Facebook, Inc.'s earnings report, available at: https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx

a. A reprimand pursuant to Article 58(2)(b); and

b. An order to bring processing operations into compliance, pursuant to Article 58(2)(d), in the terms set out at **Appendix C** hereto; and

c. An administrative fine, pursuant to Articles 58(2)(i) and 83, addressed to WhatsApp, in the amount of €225 million. For the avoidance of doubt, that fine reflects the infringements that were found to have occurred, as follows:

   i. In respect of the infringement of Article 5(1)(a) of the GDPR, a fine of €90 million;
   ii. In respect of the infringement of Article 12 of the GDPR, a fine of €30 million;
   iii. In respect of the infringement of Article 13 of the GDPR, a fine of €30 million; and
   iv. In respect of the infringement of Article 14 of the GDPR, a fine of €75 million.

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

WhatApp Ireland Limited
4 Grand Canal Square
Grand Canal Harbour
Dublin 2

Dated the 20th day of August 2021

Decision-Maker for the Commission:

[Sent electronically without signature]

_____

Helen Dixon
Commissioner for Data Protection

Appendix A – Summary of Directions and Findings

Outcome	*Summary of Outcome*	*Location within Decision*
Part 1: Transparency in the context of non-users		
Finding	Prior to lossy hashing, the phone number of a non-user constitutes the personal data of that non-user in circumstances where the non-user can be indirectly identified by reference to his/her phone number	Paragraph 105
Finding	After lossy hashing, the phone number of a non-user, constitutes the personal data of that non-user in circumstances where the non-user cannot be identified	Paragraph 110
Finding	When processing non-user data, WhatsApp does so as a data controller, and not a processor.	Paragraph 154
Finding	WhatsApp has failed to comply with its obligations to non-users pursuant to Article 14.	Paragraph 177
Part 2: Transparency in the context of users		
Finding	WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(a).	Paragraph 249
Finding	WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(b).	Paragraph 256
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c) and Article 12(1).	Paragraph 399
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(d).	Paragraph 416
Finding	WhatsApp has failed to provide the information required by Article 13(1)(e) and Article 12(1).	Paragraph 434
Finding	WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1).	Paragraph 457
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(a)	Paragraph 476
Finding	WhatsApp has complied, in full, with its obligations to provide information pursuant to Article 13(2)(b).	Paragraph 482
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1).	Paragraph 496
Finding (incorporating a Direction)	WhatsApp has broadly complied with the obligation arising pursuant to Article 13(2)(d), **subject to the direction that** WhatsApp include reference to the existence of this right under the "How You	Paragraph 503

	Exercise Your Rights" section so as to ensure that the data subject is presented with the required information in a place where he/she might expect to find it.	
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(e)	Paragraph 520
Part 3: Transparency in the context of any sharing of personal data between WhatsApp and the Facebook Companies		
Finding (incorporating a Direction)	WhatsApp has failed to comply with its transparency obligations pursuant to Articles 13(1)(c), 13(1)(d), 13(1)(e) and 12(1) in relation to how WhatsApp works with the Facebook Companies. WhatsApp has broadly complied with its obligations pursuant to Article 13(1)(d). Unless WhatsApp has a concrete plan in place, that includes a definitive and imminent commencement date, to commence the sharing of personal data on a controller-to-controller basis with the Facebook Companies for safety and security purposes, the misleading elements of the Legal Basis Notice and Facebook FAQ should be deleted to reflect the true position.	Paragraphs 591 and 592
Part 4: Article 5(1)(a) – Extent of compliance with the principle of Transparency		
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 5(1)(a)	Paragraph 595

Appendix B – Glossary of Terms

The **2018 Act**	The Data Protection Act, 2018
The **25 May Email**	The email dated 25 May 2018 from WhatsApp to the Commission
Appendix C	The list of relevant material, from the Investigator's inquiry file
The **Article 65 Decision**	The decision of the European Data Protection Board (1/2021), adopted 28 July 2021
The **Article 65 Submissions**	WhatsApp's Article 65 submissions dated 28 May 2021
The **Board** (otherwise the EDPB)	The European Data Protection Board
The **CJEU**	The Court of Justice of the EU
The **Contact Feature**	WhatsApp's contact list feature (as defined in the Response to Investigator's Questions)
The **Contact Feature Pop-Up**	The pop-up notification that issues to users to invite them to grant WhatsApp access to their device's address book (as furnished under cover of the email dated 20 March 2019 from WhatsApp to the Investigator)
The **Commission**	The Data Protection Commission
The **Composite Draft**	The Commission's composite draft decision dated 24 December 2020 (prepared for the purpose of the Article 60 process)
CSA	Concerned supervisory authority
The **Decision**	The decision dated 20 August 2021, recording the Commission's views as to whether or not an infringement of the GDPR has occurred/is occurring and the action that the Commission proposes to take, in response to any proposed finding(s) of infringement
The **Directive**	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
The **Draft Report**	The Investigator's draft inquiry report dated 30 May 2019
The **EDPB** (otherwise the Board)	The European Data Protection Board
The **Facebook Companies**	The collective term, used by the Commission, for those members of the Facebook family of companies that process, for any purpose, personal data under the controllership of WhatsApp
The **Facebook FAQ**	The FAQ available at https://faq.whatsapp.com/general/26000112/?eea=1

FAQ	Frequently Asked Question
The **Final Report**	The Investigator's final inquiry report dated 9 September 2019
The **Final Submissions**	WhatsApp's final submissions dated 19 August 2021
The **GDPR**	The General Data Protection Regulation (2016/679)
The "**How to Delete Your Account" FAQ**	The WhatsApp FAQ available at https://faq.whatsapp.com/en/general/28030012/
The "**I have Questions" FAQ**	The WhatsApp FAQ previously available at https://faq.whatsapp.com/en/general/28030012/
The **Inquiry Submissions**	WhatsApp's Submissions to the investigator's draft inquiry report, as furnished under cover of letter dated 1 July 2019
The **Legal Basis Notice**	The "How We Process Your Information" notice furnished by way of Appendix 4 to the Response to Investigator's Questions
The **Non-User List**	The list of lossy-hashed values stored on WhatsApp's servers
The **Notice of Commencement**	The Notice of Commencement of Inquiry dated 10 December 2018
Opinion 1/2010	Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted 16 February 2010 (00264/10/EN WP 169)
Opinion 3/2013	Article 29 Working Party, Opinion 3/2013 on purpose limitation, adopted 2 April 2013 (00569/13/EN WP 203)
Opinion 4/2007	Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted 20 June 2007 (01248/07/EN WP 136)
The **Page**	The suite of policies and notices set out in the form of a continuous scroll, under the heading "WhatsApp Legal Info"
The **Preliminary Draft**	The Preliminary Draft decision that issued to WhatsApp on 21 May 2020
The **Preliminary Draft Submissions**	The submissions furnished under cover of letter dated 6 July 2020, in response to the Preliminary Draft
The **Privacy Policy**	WhatsApp's Privacy Policy, last modified 24 April 2018 (as furnished by way of Appendix 2 to the Response to Investigator's Questions)
The **Proposed Approach**	The approach proposed to be taken by the Decision-Maker in relation to the interpretation of Article 13(1)(c) of the GDPR
The **Response to Investigator's Questions**	The information furnished in WhatsApp's letter of response dated 25 January 2019
SA	Supervisory authority

The **Service**	WhatsApp's internet-based messaging and calling service
The **Supplemental Draft**	The Supplemental Draft decision that issued to WhatsApp on 20 August 2020
The **Supplemental Draft Submissions**	The submissions furnished under cover of letter dated 1 October 2020, in response to the Supplemental Draft
The **Transparency Guidelines**	Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01)
WhatsApp	WhatsApp Ireland Limited

Appendix C – Terms of Order to bring processing operations into compliance, made pursuant to Article 58(2)(d)

	Action Required	***Deadline for Compliance***
1.	Take the action required such that the information prescribed by Article 14 is provided to those non-users whose personal data is being processed by WhatsApp. When doing so, WhatsApp must ensure that the information is provided in a manner that complies with the requirements of Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of this Decision (and, in particular, paragraphs 163, 164, 166 and 167).	The period of 3 months, commencing on the day following the date of service of this order
2.	Take the action required to provide the information prescribed by Article 13(1)(c) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of the Decision. The information to be provided, in this regard, and the manner in which it should be provided, is detailed in paragraphs 301 to 302 and 325 to 399 and 539 to 592 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
3.	Take the action required to provide the information prescribed by Article 13(1)(d) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of the Decision, in particular paragraphs 411 to 416 and 539 to 592 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
4.	Take the action required to provide the information prescribed by Article 13(1)(e) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of the Decision. The information to be provided, in this regard, and the manner in which it should be provided, is detailed in paragraphs 422 to 434 and 539 to 592 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
5.	Take the action required to provide the information prescribed by Article 13(1)(f) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision. The information to be provided, in this regard, and the manner in which it should be provided, is detailed in paragraphs 443 - 457 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
6.	Take the action required to provide the information prescribed by Article 13(2)(a) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision. The deficiencies to be remedied, in this regard, are detailed in paragraphs 464 – 476 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order

6.	Take the action required to provide the information prescribed by Article 13(2)(c) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision. The deficiencies to be remedied, in this regard, are detailed in paragraphs 486 - 496 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
7.	Take the action required to provide the information prescribed by Article 13(2)(e) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision and, in particular, paragraphs 507 to 520.	The period of 3 months, commencing on the day following the date of service of this order
8.	Take the action required to incorporate reference to the existence of the right to lodge a complaint with a supervisory authority in the "How You Exercise Your Rights" section of the Privacy Policy.	The period of 3 months, commencing on the day following the date of service of this order

Appendix D – The Article 65 Decision