

In the matter of the General Data Protection Regulation

DPC Inquiry Reference: IN-18-5-6

**In the matter of JG, a complainant, concerning a complaint directed against WhatsApp Ireland Limited
in respect of the WhatsApp Service**

**Decision of the Data Protection Commission made pursuant to Section 113 of the Data Protection Act,
2018 and Articles 60 and 65 of the General Data Protection Regulation**

**Further to a complaint-based 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 12th day of January 2023



Data Protection Commission

21 Fitzwilliam Square South
Dublin 2, Ireland

1. INTRODUCTION AND PROCEDURAL BACKGROUND

PURPOSE OF THIS DOCUMENT

1.1 This document is a decision (“the **Decision**”) of the Data Protection Commission (“the **Commission**”), made in accordance with Section 113 of the Data Protection Act 2018 (“the **2018 Act**”), arising from an inquiry conducted by the Commission, pursuant to Section 110 of the 2018 Act (“the **Inquiry**”).

1.2 The Inquiry, which commenced on 20 August 2018, examined whether WhatsApp Ireland Limited (“**WhatsApp**”) complied with its obligations under the EU General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council) (“the **GDPR**”) in respect of the subject matter of a complaint made by Mrs. ■■■ (“the **Complainant**”). The complaint was referred to the Commission by the Hamburg Data Protection Authority: *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (“the **Hamburg DPA**”) on 25 May 2018 (“the **Complaint**”). The Hamburg DPA subsequently passed the Complaint to the German Federal Data Protection Authority, the relevant national authority: *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* (“the **German Federal DPA**”). The Complainant is at all times represented by noyb – European center for digital rights.

1.3 This Decision further reflects the binding decision that was made by the European Data Protection Board (the “**EDPB**” or, otherwise, the “**Board**”), pursuant to Article 65(2) of the GDPR¹ (the “**Article 65 Decision**”), which directed changes to certain of the positions reflected in the draft decision that was presented by the Commission for the purposes of Article 60 GDPR (“the **Draft Decision**”) as detailed further below. The Article 65 Decision will be published on the website of the EDPB, in accordance with Article 65(5) of the GDPR, and a copy of same is attached at Schedule 2 to this Decision.

1.4 Further details of procedural matters are set out in Schedule 1 to this Decision.

2. FACTUAL BACKGROUND AND THE COMPLAINT

FACTUAL BACKGROUND

2.1 WhatsApp is an online instant messaging platform. In order to access the WhatsApp service, a prospective user must create a WhatsApp account. To create a WhatsApp account, a prospective user is required to accept a series of terms and conditions, referred to by WhatsApp as its Terms

¹ Binding Decision 5/2022 on the dispute submitted by the Irish SA on WhatsApp Ireland Limited, adopted 5 December 2022

of Service (the “**Terms of Service**”). When a prospective user accepts the Terms of Service, the terms contained therein constitute a contract between the (new) user and WhatsApp. It is only on acceptance of the Terms of Service that the individual becomes a registered WhatsApp user.

2.2 In April 2018, WhatsApp updated the Terms of Service to give effect to changes it sought to implement to comply with the obligations which would arise when the GDPR became applicable from 25 May 2018. Obligations introduced by the GDPR include, *inter alia*, a requirement that organisations processing personal data have a lawful basis for any such processing. Legal bases provided for in the GDPR include consent of the data subject, necessity based on the requirement to fulfil a contract with the data subject or processing based on the legitimate interests of the data controller. In addition, such organisations are required to provide detailed information to users at the time personal data is obtained in relation to the purposes of any data processing and the legal basis for any such processing. In essence, there must be a legal basis for each processing operation or sets of operations (of personal data) and there are transparency requirements in respect of the communication of such information to individual users.

2.3 To continue to access the WhatsApp service, all users were required to accept the updated Terms of Service prior to 25 May 2018. The updated Terms of Service were brought to the attention of existing users by way of a series of information notices and options, referred to as an “engagement flow” or “user flow”. The engagement flow was designed to guide users through the processing of accepting the updated Terms of Service; the option to accept the updated “terms” was presented to users at the final stage of the engagement flow. As referenced in the full text of the Terms of Service, a separate Privacy Policy provides information to users on WhatsApp’s processing of personal data in respect of the service.

2.4 Existing users were not provided with an opportunity to disagree and continue to use the service, to copy their account, or to delete their account. The only available choice was to accept the Terms of Service, stop using the app or uninstall the app.²

2.5 Figures 2.1 below is a screenshot of the final stage of the “engagement flow” which brought an existing user, the Complainant, through the process of accepting the updated Terms of Service. The screenshot is in German; an English translation can be found below.

² Complaint, paragraph 1.4.



Figure 2.1

2.6 An English translation (via machine-translation) of the text is as follows:

Figure 2.1: “Welcome to WhatsApp! Click “Agree and continue” to accept the WhatsApp Terms of Service and the Privacy Policy”

OVERVIEW OF THE COMPLAINT

2.7 The Complaint was made in the context of WhatsApp’s updated Terms of Service and the requirement for existing users to accept in accordance with the above formulation or to no longer have access to the service.

2.8 In respect of the updated Terms of Service, the Complainant argues that she was given a binary choice: either accept the Terms of Service and the associated Privacy Policy by selecting the “accept”

button,³ or cease using the service. The Complainant's argument is predicated on the Data Policy being incorporated into the Terms of Service. This claim is disputed by WhatsApp.⁴ The Complainant further alleges that WhatsApp relied on "forced consent" to process personal data on the basis that "*the controller required the data subject to agree to the entire privacy policy and the new terms*"⁵ and did not give users a genuine choice to decline the updated terms without suffering detriment.

2.9 In addition, the Complainant alleges that it is unclear which specific legal basis is being relied on by the controller for each processing operation. Indeed, she argues that "[i]t remains, nevertheless, unclear which exact processing operations the controller chooses to base on each specific legal basis"⁶ as "[t]he controller simply lists all six bases for lawful processing under Article 6 of the GDPR in its privacy policy without stating exactly which legal basis the controller relies upon for each specific processing operation."⁷ In connection with this, the Complainant expresses particular concern about reliance on Article 6(1)(b) GDPR as a legal basis for the processing operations detailed in the Terms of Service; extracts from the Terms of Service which relate to these processing operations are found below.

2.10 As the GDPR requires controllers to provide detailed information to users at the time when personal data are obtained, including the provision of information about the purposes of the processing as well as the legal bases for the processing, the Complainant argues that this lack of information breaches the transparency obligations in the GDPR.⁸

2.11 The sections of the Terms of Service (in the form that existed as at the date the Complaint was made) that relate to the data processing complained of are as follows:

"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

³ For completeness, it should be noted that WhatsApp disputes the claim that the Privacy Policy is part of the Terms of Service, or that the Complainant "consented" to the Privacy Policy in the sense meant by Article 6(1)(a) GDPR.

⁴ WhatsApp submissions on Draft Inquiry Report, paragraphs 2.1-2.5.

⁵ Complaint, paragraph 1.3.

⁶ *Ibid.*

⁷ For completeness, it should be noted that the legal bases for processing of personal data include consent of the data subject, necessity based on the requirement to fulfil a contract with the data subject or processing based on the legitimate interests of the data controller. There is no hierarchy as between these legal bases set down in the GDPR.

⁸ The Complaint, paragraph 2.3.1.

Inc. (collectively, "WhatsApp," "our," "we," or "us") that provides the services described below to you (collectively, "Services")::

Privacy And Security Principles. *Since we started WhatsApp, we've built our Services with strong privacy and security principles in mind.*

Connect you with people and organizations you care about

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 policies [here](#).

SCOPE OF THE COMPLAINT

2.12 I have carried out my assessment of the scope of the Complaint to the extent that it relates to specified data processing and specified alleged infringements of the GDPR. A chronology of issues that arose (1) as between the parties, and (2) as between the parties and the Commission, in the course of establishing the substantive scope of the Complaint, is included in Schedule 1. Also included in Schedule 1 are details of the approach I adopted in determining the issues raised. In determining the precise parameters of the scope of the Complaint, I had regard, in the Draft Decision, to the Complaint as a whole and, in particular, took note of the express statements in the Complaint which define its scope. I also had regard, in the Draft Decision, to the Investigator's analysis in respect of the scope of the Complaint.

2.13 On his assessment of the Complaint, the Investigator concluded that there were four key issues to be analysed in the context of his Inquiry:⁹

- a) Whether the data subject's acceptance of WhatsApp's Terms of Service, and/or Privacy Policy should/must be construed as the provision of consent (within the meaning of Articles 4(11) and 6(1)(a) GDPR) to processing described in those documents.¹⁰
- b) Whether WhatsApp is prohibited from relying on Article 6(1)(b) GDPR as a lawful basis for processing of personal data with respect to its service.¹¹
- c) Whether WhatsApp misrepresented the legal basis for processing in a manner that caused the Complainant to believe the processing was based on consent.¹²

⁹ Investigator's final inquiry report, paragraph 90.

¹⁰ *Ibid.*

¹¹ *Ibid.*

¹² *Ibid.*

- d) Whether WhatsApp failed to provide the necessary information regarding its legal basis for processing in connection with its Terms of Service and Privacy Policy.¹³
- 2.14 In the Preliminary Draft, I agreed with the Investigator’s summary of the core issues in respect of issues (a) and (b). In respect of issues (c) and (d), however, I took a different view.
- 2.15 Issue (c), as identified by the Investigator, solely addresses the allegation that WhatsApp has misrepresented the lawful basis relied on in connection with the Terms of Service. In the Preliminary Draft, I agreed that this issue falls within the scope of the Complaint. Issue (d), however, was treated by the Investigator as a generalised assessment of whether WhatsApp’s Privacy Policy complies with Article 13(1)(c) GDPR as a whole with regard to processing conducted on foot of Article 6(1)(b) GDPR. This is based on the fact that the Complaint states, in generalised terms, that:

“It remains, nevertheless, unclear which exact processing operations the controller chooses to base on each specific legal basis under Article 6 and Article 9 of the GDPR.

In its updated privacy policy, the controller simply lists all six bases for lawful processing under Article 6 of the GDPR in its privacy policy without stating exactly which legal basis the controller relies upon for each specific processing operation.”¹⁴

- 2.16 It is on that basis that the Investigator interpreted the scope of the Complaint as comprising the allegation that the Privacy Policy breaches Article 13(1)(c) GDPR. It is crucial, however, to view the above quotation in the context of the subsequent statement, which says:

“In any case, the controller required the data subject to “agree” to the entire privacy policy and to the new terms.

It is therefore impossible to determine, which exact processing operations are based on each specific legal basis under Article 6 and 9 of the GDPR.

This leads to our preliminary assumption, that all processing operations described therein are based on consent, or that the controller at least led the data subject to believe that all these processing operations are (also) based on Article 6(1)(a) and/or 9(2)(a) of the GDPR.”¹⁵

¹³ *Ibid.*

¹⁴ Complaint, paragraph 1.3.

¹⁵ *Ibid.*

2.17 I do not accept that the factual question of whether WhatsApp “misled” the data subject (i.e. issue (c)) is a separate legal question from whether WhatsApp complied with its transparency

obligations in the context of processing allegedly carried out pursuant to Article 6(1)(b) GDPR (i.e. issue (d)). There is no distinct legal issue raised by the question whether, as a matter of fact, the Complainant did or did not believe that the processing was based on Article 6(1)(a) GDPR (i.e. consent) and not on Article 6(1)(b) GDPR (i.e. necessity for the performance of a contract). If WhatsApp has breached its transparency obligations, it logically follows that the Complainant will have been unlawfully “misled”, whether deliberately or otherwise. If WhatsApp has complied with its transparency obligations, it cannot be the case that the Complainant was unlawfully misled. On that basis, my view is that issues (c) and (d) are essentially concerned with the same issue. WhatsApp expressed agreement with this analysis in its submissions on the Preliminary Draft of this decision (“the Preliminary Draft”).¹⁶

- 2.18 In its submissions on the draft inquiry report prepared by the Investigator (“the Draft Inquiry Report”), the Complainant’s representative submitted that the Commission “*in no way investigated why specific parts of the terms of service should be a contract*”¹⁷ and argued, therefore, that the investigation is somehow incomplete. I expressed the view, in the Draft Decision, that such an inquiry would be unnecessary in order to resolve the core issue in dispute here, and would not divulge any new information or serve a useful purpose at this stage. As is set out in Section 3, below, there is no dispute as to the existence of a contract between WhatsApp and the Complainant or the fact that no consent within the meaning of the GDPR has been provided by the Complainant in concluding the “agreement” in dispute. What is in dispute, as set out in detail in this Decision and in Schedule 1, is the lawfulness of the personal data processing and the transparency of the information provided.
- 2.19 Following the circulation of the Draft Decision to the supervisory authorities concerned for the purpose of enabling them to express their views in accordance with Article 60(3) GDPR, the supervisory authorities of Finland, France and Italy raised objections in relation to the Commission’s assessment of the scope of the Complaint, as summarised above.

Having considered those objections, the EDPB determined, at paragraph 218 of the Article 65 Decision, that the inquiry underpinning this Decision ought to have included an examination of “*the legal basis for [WhatsApp’s] processing operations for the purposes of behavioural advertising, the potential processing of special categories of personal data, applicable legal basis for provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements, as well as the processing of personal data for the purposes of marketing.*” Accordingly, the EDPB directed, at paragraph 222 of the Article 65 Decision, the Commission to commence a new Inquiry into “*WhatsApp IE’s processing operations in its service in order to determine if it processes special categories of personal data (Article 9 GDPR), processes data for the purposes of behavioural advertising, for marketing purposes, as well as for the provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements, and in order to determine if it*

¹⁶ WhatsApp submissions on the Preliminary Draft, paragraph 8.2.

¹⁷ Complainant submissions on Draft Inquiry Report, paragraph 3.1.2.

complies with the relevant obligations under the GDPR.” While that direction cannot be addressed by the Commission in this Decision, the Commission considers it necessary to note the position, in light of the Commission’s assessment of the scope of the Complaint (as already recorded above) and for the purpose of ensuring compliance with its obligation, pursuant to Article 65(6) GDPR, to adopt its final decision on the basis of the Article 65 Decision.

2.20 On the basis of the above, the issues that I addressed in the Draft Decision were as follows:

- Issue 1 – Whether clicking on the “accept” button constitutes or must be considered consent for the purposes of the GDPR
- Issue 2 – Reliance on Article 6(1)(b) as a lawful basis for personal data processing
- Issue 3 – Whether WhatsApp provided the requisite information on the legal basis for processing on foot of Article 6(1)(b) GDPR and whether it did so in a transparent manner.

2.21 The Draft Decision proposed a number of findings, by reference to the issues identified above. The first of those findings proposed a determination that WhatsApp: (a) has not sought to rely on consent in order to process personal data to deliver the Terms of Service, and (b) is not legally obliged to rely on consent in order to do so (“Finding 1”). Finding 1, therefore, constituted a proposal in the Draft Decision to dismiss/reject an aspect of the Complaint.

2.22 The Article 65 Decision does not contain any instruction or direction that would require (or permit) the Commission to disturb proposed Finding 1. Accordingly, Finding 1 remains part of the decision that fell to be adopted, following the conclusion of the Article 65 process. Article 60(9) GDPR provides, in this regard, that:

“Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.”

2.23 Given that Finding 1 represented the dismissal/rejection of part of the Complaint, it was necessary for the Commission to remove the finding and its supporting analysis from this Decision prior to its adoption in circumstances where Article 60(9) GDPR requires this to be adopted, by way of a separate decision, by the supervisory authority of the Complainant (as identified in paragraph 1.2, above).

2.24 Accordingly, the following is an analysis of Issues 2 and 3 (in circumstances where Issue 1 is the subject of Finding 1 and has therefore been removed from this Decision prior to its adoption for the reasons outlined above).

3 ISSUE 2 - RELIANCE ON 6(1)(B) AS A LAWFUL BASIS FOR PERSONAL DATA PROCESSING

3.1 As set out above, the Complainant contends that WhatsApp’s processing of personal data under the Terms of Service must be based entirely on consent as a legal basis under the GDPR. I note that there is no hierarchy of legal bases in the GDPR and there is nothing to support the contention that the agreement in question must legally be based on consent. The Complainant’s argument also rests on the contention that WhatsApp cannot rely on Article 6(1)(b) GDPR to process personal data in order to perform the Terms of Service.

3.2 In considering this issue, I will first address the relationship between the Terms of Service and the Privacy Policy. This assessment is necessary as the Complainant argues that she “agreed” to the Privacy Policy by accepting WhatsApp’s updated Terms of Service. WhatsApp has argued that this position is not correct. After coming to a conclusion on this matter, I will then consider the substantive question of whether WhatsApp is entitled to rely on Article 6(1)(b) GDPR as a lawful basis for the processing of personal data.

THE RELATIONSHIP BETWEEN THE TERMS OF SERVICE AND PRIVACY POLICY

3.3 The Complainant alleges that in clicking the “accept” button, she agreed to both the Privacy Policy and the Terms of Service and that the alleged non-compliance is compounded by such agreement to both. In examining this aspect of the Complaint, the Investigator was of the view that that the Privacy Policy was not a component of the data subject’s contract with WhatsApp. The Investigator also acknowledged, in the final inquiry report (“the **Final Inquiry Report**”) that the Complainant seems to have conceded that there is no “consent” and therefore no “agreement” to the Privacy Policy. I have set this out in more detail above, with specific regard to the argument that users were asked to “accept” both documents. The Investigator ultimately found that, given the conditions for consent were not met, and given the contents of the Privacy Policy made clear that any such “consent” to the Privacy Policy would be contradictory, this acceptance was not consent.¹⁶

3.4 I note therefore the Investigator’s consideration of whether the Complainant was forced to consent to all of the processing operations set out in the Privacy Policy. In the Draft Decision, I expressed the view that the acceptance in question was not an act of consent but, on its terms, constituted acceptance of a contract i.e. acceptance of the Terms of Service. Although the Privacy

¹⁶ Final Inquiry Report, paragraphs 180-182.

Policy was contained within the engagement flow, I am not satisfied that it was thereby incorporated into the Terms of Service. WhatsApp has stated that it *“agrees with the Commission’s assessment in this regard”*.¹⁷

3.5 The Privacy Policy is a document through which WhatsApp seeks to comply with particular provisions of the GDPR in relation to transparency, whereas the Terms of Service is a contract. WhatsApp relies on various legal bases for various data processing operations, some of which are based on consent and some of which are based on contractual necessity. Where contractual necessity is relied on, the contract in question is the Terms of Service. At this juncture, I am merely expressing the view that the contract in question, and therefore the contract for which the analysis based on Article 6(1)(b) GDPR must take place, is the Terms of Service only. The Privacy Policy is only relevant insofar as it sheds light on the processing operations carried out for which WhatsApp relies on Article 6(1)(b) GDPR. It is essentially an explanatory document. The extent to which it does shed light on these processing operations, i.e. matters of transparency, are relevant only to the next matter to be addressed in this Decision.

3.6 I also note that, while the Complaint refers to various examples of data processing, e.g. advertising, it does not go so far as to directly link the Complaint to specific processing operations by reference to an identifiable body of data with any great clarity or precision. In the circumstances, I expressed the view, in the Draft Decision, that the issue surrounding Article 6(1)(b) GDPR in the Complaint ought to be considered at the level of principle, with my findings to be made on that basis. The Privacy Policy itself references a very wide range of processing operations. Within the framework of this Complaint, there has not been a high degree of specificity in relation to individual processing operations complained of. I also note, as I have in Schedule 1, that the Complainant’s representative sought to direct the Commission to conduct an assessment of all processing operations carried out by WhatsApp. I have set out why, in my view, it is not open to a complainant or their representative to demand such an activity. More generally, I have also already indicated that, in my view, complaints should have a reasonable degree of specificity.

3.7 The Complaint does, however, focus on a number of particular processing activities and has a specific focus on data processed to facilitate improvements to services and advertising. This was accordingly the focus of the Draft Decision. To ensure that this Inquiry has a reasonable degree of specificity, the Draft Decision proposed to decide whether WhatsApp can, in principle, rely on Article 6(1)(b) GDPR for processing under the contract, including and in particular in the context of service improvements, providing metrics to third parties (such as companies within the same group of companies), and advertising.

3.8 On the question of advertising, I expressed the view, in the Draft Decision, that no evidence has been presented by the Complainant that WhatsApp processes personal data for the purpose of advertising and relies on Article 6(1)(b) GDPR to do so. The Investigator correctly pointed out in

¹⁷ WhatsApp submissions on Preliminary Draft, paragraph 7.8.

the Final Inquiry Report that “WhatsApp’s Terms of Service bear little resemblance to the examples cited in the complaint of situations where Article 6(1)(b) does not apply”,¹⁸ such as advertising and sponsored content. Given the absence of such references in WhatsApp’s Terms of Service, and the absence of evidence that such processing takes place, I agreed with the Investigator, in my Draft Decision, that arguments relating to the applicability of Article 6(1)(b) GDPR to data processing to facilitate advertising were not relevant to the within Inquiry. WhatsApp has stated in its submissions on the Preliminary Draft that it “agrees with the Commission’s approach that the issue of advertising is irrelevant to the Inquiry”.¹⁹ As already noted at paragraph 2.19, above, the EDPB disagreed with this view in the Article 65 Decision.

THE COMPLAINT, THE SUBMISSIONS OF THE PARTIES ON THE FINAL INQUIRY REPORT, AND THE FINAL INQUIRY REPORT

3.9 The Complainant argues that WhatsApp is not entitled to rely on Article 6(1)(b) GDPR, i.e. contractual necessity, as a legal basis. The Complainant contends that WhatsApp could only rely on Article 6(1)(b) GDPR in respect of processing that is “strictly necessary” to perform the contract, and that such processing must be linked to “core” functions of the contract. To support this view, the Complainant relies on Opinion 06/2014 of the Article 29 Working Party which recommended that “[t]he contractual necessity lawful basis must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller”.²⁰²¹

3.10 Specifically, the Complainant argues that instant messaging and video calls constitute a “core” element of WhatsApp’s contract, but data collected to facilitate improvements to services do not. The Complainant’s position is premised on the idea that there is an identifiable “purpose” or “core” of each contract which is discernible by reference to the contract as a whole and the intention of the parties (as opposed to being strictly limited to the text of the contract). The Complainant is therefore asking that an assessment of the Terms of Service be carried out to determine what the “core” purpose of the contract is. It would follow from the Complainant’s position that any processing that is not strictly necessary to fulfil these “core” purposes or objectives, cannot be carried out on foot of Article 6(1)(b) GDPR.

3.11 As a preliminary matter, I emphasise my view that issues of interpretation and validity of national contract law are not directly within the Commission’s competence. Nonetheless, it is important to note that the legal concept of a “purpose” or “core” of a contract is one more often found in civil law jurisdictions. The Commission’s role is in any event limited to interpreting and applying

¹⁸ Final Inquiry Report, paragraph 226.

¹⁹ WhatsApp submissions on Preliminary Draft, paragraph 7.5.

²⁰ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive

²¹ /46/EC, page 16, https://ec.europa.eu/justice/article-29/documentation/opinionrecommandation/files/2014/wp217_en.pdf.

the GDPR and, in interpreting and applying Article 6(1)(b) GDPR specifically, it must always be borne in mind that the Commission is not competent to rule directly on matters of national contract law or to determine questions of the general validity of a contract.

3.12 I note that the Complainant also explicitly sought to have the Commission investigate and make findings in respect of contract and consumer law. I agree with the position of the Investigator that this falls outside the remit of a supervisory authority under the GDPR. I further note that the Investigator correctly drew the Complainant's attention to the relevant Irish and German consumer and competition authorities, which have competence in this regard. It seems to me that these legal regimes would be a more appropriate avenue for the Complainant to ventilate the issues surrounding contract law referred to above.

3.13 The Complainant argues that the "Our Services" section of the Terms of Service "*often reads more like a description and similar to an advertising brochure or a data protection declaration in the meaning of Article 13 or 14 GDPR.*"²² The Complainant also argues that showing any user advertisements is a "purely factual" rather than a contractual obligation or duty.²³ In addition, the Complainant's argument endeavours to draw a distinction between "implicit consent" – i.e. some form of agreement that is implicit or obvious within a contract for services – and "*the part of the contract that is objectively to be regarded as circumvention of consent*" – i.e. consent which is made contingent on the acceptance of a contract.²⁴ Applying the narrow interpretation of Article 6(1)(b) GDPR that is proposed by the Complainant, the argument is that the processing required to deliver the "factual" services set out in the contract cannot fall within Article 6(1)(b) GDPR. This rests on the aforementioned distinction drawn by the Complainant between processing that is strictly necessary to deliver the "core" objectives of the service i.e. providing a messaging service, and factual events simply mentioned or described in the contract i.e. using data to improve a service.

3.14 The remaining argument is that the "take it or leave it" approach to signing up or continuing to use WhatsApp in any event does not constitute processing that is permitted by Article 6(1)(b) GDPR. To assess whether this interpretation of Article 6(1)(b) GDPR is correct, I must first consider whether the processing which is carried out on foot of the acceptance of the contract is necessary to perform that contract. In essence, this requires an assessment of whether the services offered by WhatsApp pursuant to the contract are necessary to fulfil the contract's core functions.

3.15 In advancing the argument that Article 6(1)(b) GDPR can only be relied on to legitimise data processing that constitutes "a core element" of the service,²⁵ the Complainant relies on guidance

²² The Complainant's submissions on Draft Inquiry Report, paragraph 3.1.1.2.

²³ *Ibid*, paragraph 3.1.3.

²⁴ *Ibid*, Paragraph 4.4.3.6.

²⁵ Complaint, paragraph 1.3.

of the EDPB. Moreover, the Complainant argues that, *inter alia*, WhatsApp has made a “*ridiculous argument*” in arguing that a user can “agree” to data processing for Terms of Service that primarily involve the processing of data.²⁶

3.16 The Complainant is therefore of the view that this particular interpretation should be applied to the circumstances of the Complaint by conducting an assessment as to what constitutes the “core” of the contract between the user and WhatsApp. The argument is that any services (such as, in the Complainant’s view, improvements) which do not form part of the activities which are strictly necessary to fulfil the core objective of the contract cannot be rendered lawful by Article 6(1)(b) GDPR.

3.17 Put very simply, the Complainant is advancing a narrow and purpose-based interpretation of Article 6(1)(b) GDPR, that argues that the data processing should be the least invasive processing possible in order to fulfil the objective of the contract (here, what the overall contract sets out to do, rather than only what the contract says). In contrast, WhatsApp is advancing a broader interpretation that facilitates a certain degree of contractual freedom in relation to how broad the data processing might be, provided that the processing is in fact necessary to perform a term of the specific contract.

3.18 WhatsApp argues that there is no basis to contend that WhatsApp, in clearly relying on a contract with the user, has attempted to mislead the user and to “infer” consent from a user. WhatsApp’s position is that the condition of necessity for contractual performance in “*Article 6(1)(b) GDPR does not mean that processing must be strictly essential to the performance of the contract, or the only way to perform the underlying contract.*”²⁷ WhatsApp emphasises that, rather than being required to use the most minimal processing possible in order to perform the contract, contractual freedom must allow the parties to exercise a certain element of agency in coming to an agreement, even where that agreement might involve the delivery of a service primarily using data processing. WhatsApp’s position is therefore that the Complainant’s interpretation (and proposed application) of the GDPR is incorrect and excessively narrow. It referred to and relied on these submissions in its submissions on the Preliminary Draft.²⁸

3.19 WhatsApp also argues that there is an absence of meaningful rationale in the Complaint as to why any of the elements of its service described in Section 1 of its Terms of Service cannot be based on Article 6(1)(b) GDPR. It submits that “*the processing which is necessary to perform the full agreement entered into between the parties can include optional or conditional elements of contract and this is a matter for the parties to the contract*”.²⁹ WhatsApp’s position is that the Commission should apply a broader interpretation of Article 6(1)(b) GDPR, such that processing

²⁶ Complainant submissions on Draft Inquiry Report, paragraph 4.3.

²⁷ WhatsApp submissions on Draft Inquiry Report, paragraph 4.2.

²⁸ WhatsApp submissions on Preliminary Draft, paragraph 7.10.

²⁹ WhatsApp submissions on Draft Inquiry Report 29 July 2019, paragraph 4.3.

that is necessary to deliver a contract can be lawful irrespective of whether the specific processing is essential, or the most minimal way, to deliver the service. In its submissions on the Preliminary Draft, WhatsApp once again emphasised its position that processing that is necessary for the performance of a contract “*does not mean that processing must be essential to the performance of the contract or the only way to perform the underlying contract.*”³⁰

3.20 The Investigator acknowledged the difficulties in interpreting contractual necessity *in vacuo*, where there is limited harmonisation of contract law at European level and where the Commission is not competent to rule on matters of contract law.³¹ The Investigator expressed particular doubts about applying a test based on what is necessary to fulfil the core functions/objectives of a contract given the lack of certainty surrounding it.³² The Investigator concluded that the concept of necessity in Article 6(1)(b) GDPR “*includes processing which is necessary to perform the full agreement entered into between the parties, including optional or conditional elements of contract*”.³³

3.21 The Investigator’s position is in contrast to that of the Complainant, which is that “necessity” should be assessed strictly by reference to its meaning as an element in the proportionality test in applying Article 52(1) of the European Charter of Fundamental Rights and Freedoms (“the **Charter**”), i.e. that the measure be strictly necessary in order to fulfil the objective.

WHETHER WHATSAPP CAN RELY ON ARTICLE 6(1)(B) GDPR

3.22 In coming to a conclusion on this matter in the Preliminary Draft, I had regard to the Guidelines of the EDPB on processing for online services based on Article 6(1)(b) GDPR; while these Guidelines are not strictly binding, there are nonetheless instructive in considering this issue. The Guidelines state in clear terms that “*the processing in question must be objectively necessary for the performance of a contract with a data subject*”.³⁴ In my view, this turns on a consideration of what is meant by the concepts of “performance”, “necessity” and “contract”, as understood in the context of data protection law.

3.23 It is, in the Commission’s view, important to have regard not just to the concept of what is “necessary”, but also to the concept of “performance”. The EDPB has set out that controller should ensure “*that processing is necessary in order that the particular contract with the data subject can be performed.*”³⁶ A contract is performed when each party discharges their contractual

³⁰ WhatsApp submissions on Preliminary Draft, paragraph 7.10.

³¹ Final Inquiry Report, paragraph 223.

³² *Ibid.*

³³ *Ibid.*, paragraph 224.

³⁴ 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 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-badopted_after_public_consultation_en.pdf, paragraph 22. ³⁶ *Ibid.*, paragraph 26.

obligations as has been agreed by reference to the bargain struck between the parties. It follows that what is “necessary” for the performance of a contract is anything that, if it did not take place, would mean the specific contract had not been performed. In this regard, I note that the mere inclusion of a term in a contract does not necessarily mean that it is necessary to perform the particular contract. This understanding is consistent with the EDPB Guidance which states that the processing will be necessary for the performance of a contract if “*the main subjectmatter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur*”.³⁵ It remains the view of the Commission, however, that necessity cannot be considered entirely in the abstract, and regard must be had for what is necessary for the performance of the specific contract freely entered into by the parties.

3.24 The EDPB states that there is:

“...a distinction between processing activities necessary for the performance of a contract, and terms making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract. ‘Necessary for performance’ clearly requires something more than a contractual condition” [my emphasis].³⁶

3.25 The Guidelines also set out that controller should:

“demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract.”³⁷

3.26 On the question of necessity, I note that the EDPB has stated that the meaning of necessity as understood in EU law must be considered when having regard to a provision of EU law, including data protection law.³⁸ This is an uncontroversial statement. I also note that in *Heinz Huber v Bundesrepublik Deutschland*, the CJEU held in the context of Directive 95/46 that necessity is an existing principle of EU law that must be interpreted in a manner that “*reflects the objective of that directive*”.^{39,40} It is important to highlight, as the Investigator has,⁴¹ that in the same case the

³⁵ *Ibid*, paragraph 30.

³⁶ Guidelines 2/2019, paragraph 27.

³⁷ *Ibid*, paragraph 30.

³⁸ *Ibid*, paragraph 23.

³⁹ Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 18 December.

⁴⁰ , para. 52.

⁴¹ Final Inquiry Report, paragraph 202(vi).

CJEU held that processing beyond the most minimal to meet the objective will still meet the necessity test if it renders a lawful objective “more effective”.⁴² However, the EDPB proposes clear limits to this by stating “*merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b).*”⁴³

3.27 The EDPB Guidelines assess necessity by reference to the “core” function of the contract. This is supportive of the Complainant’s position that the “core” functions of a contract must be assessed in order to determine what processing is objectively necessary in order to perform it. I agree with this assessment for the reasons set out by the EDPB. In this vein, I would add that the Commission’s view is that necessity is to be determined by reference to the particular contract as between the parties. Indeed, the question to be asked is whether the processing operation(s) is/are necessary to fulfil the “*specific*”⁴⁴ or “*particular*”⁴⁵ contract with the data subject. This is the view taken by the EDPB and, as Article 6(1)(b) GDPR clearly refers to the specific contract between a data controller and a data subject, I am in agreement with the EDPB in this regard.

3.28 WhatsApp submitted, in response to the Preliminary Draft, that necessity should be determined not in a general sense but based on an assessment of the contract itself. It also adds that “*the Core Functions Assessment is fully consistent with broader data protection principles...beyond simply considering if the relevant processing is referenced in the terms of the contract, but instead assesses whether that processing is integral to delivering the contractual service*”.⁴⁶ It is therefore in agreement with an assessment of a contract in the manner proposed. The Complainant made no further submissions in this regard in response to the Preliminary Draft.

3.29 In accordance with the EDPB Guidelines, and as set out in WhatsApp’s submissions referred to above, the processing in question must be more than simply the processing of personal data which is referenced in the terms of the contract. Rather, it must be necessary in order to fulfil the clearly stated and understood objectives or “core” of the contract. The “core functions” cannot, however, in the Commission’s view, be considered in isolation from the meaning of “performance”, the meaning of “necessity” as set out above, and the content of the specific contract in question. The question is therefore not what is necessary to fulfil the objectives of “messaging service” in a general sense, but what is necessary to fulfil the core functions of the particular contract between WhatsApp and WhatsApp users. In order to carry out this assessment, it is therefore necessary to consider the contract itself.

⁴² *Huber v Deutschland*, paragraph 62.

⁴³ Guidelines 2/2019, paragraph 27.

⁴⁴ *Ibid*, paragraph 30.

⁴⁵ *Ibid*, paragraph 26.

⁴⁶ WhatsApp submissions on Preliminary Draft, paragraph 7.13.

3.30 I recall my earlier statement that matters of national contract law are outside the scope of the Commission.⁴⁷ Nonetheless, for the purposes of data protection law, I note that the EDPB indicates that, in such an assessment, “*regard should be given to the particular aim, purpose, or objective of the service*”.⁴⁹ In my view, when examining what constitutes a “contract” for the purposes of Article 6(1)(b) GDPR, the term “contract” does not necessarily refer to the entirety of the (written) agreement between the parties. Rather, I agree that the correct approach is to examine the actual bargain which has been struck between the parties and determine the core function of the contract by reference to this. Therefore, the inclusion of a term which does not relate to the core function of the contract could not be considered necessary for its performance.

3.31 As an aid to deciding whether Article 6(1)(b) GDPR is an appropriate lawful basis, and in particular in considering the scope of the relevant contract, the EDPB suggests asking:

- “*What is the nature of the service being provided to the data subject?*”
- “*What are its distinguishing characteristics? What is the exact rationale of the contract (i.e. its substance and fundamental object)?*”
- “*What are the essential elements of the contract?*”
- “*What are the mutual perspectives and expectations of the parties to the contract?*”
- “*How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect?*”⁵⁰

3.32 In considering this particular issue in the context of the Complaint, it is necessary to identify the “core” functions of the contract between WhatsApp and WhatsApp users. At this point, I note that the Complaint itself does not specify, with any great precision, the extent of the processing (or indeed the processing operation(s)) that the Complainant believes to not be necessary to perform the Terms of Service. The Complainant has however made some specific submissions arguing processing for service improvement, security, “exchange of data with affiliated companies” and the processing of special category data is not necessary in order to fulfil the “core function” of a messaging and calling service. As a result, I focused on this processing in the Preliminary Draft, and retain this focus in this section of this Decision.

3.33 In the Schedule to the Draft Decision, I expressed the view that there was no evidence to support the assertion that WhatsApp is processing data that facilitates the inferring of

⁴⁷ In this regard, I also note that national contract law of individual Member States applies various standards to determine when a contract will be deemed to be performed, what contractual terms can be breached without the entire contract being deemed to be breached, and indeed how something can be deemed a “term” in the first place.

⁴⁹ 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 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-badopted_after_public_consultation_en.pdf, paragraph 30. ⁵⁰ *Ibid*, paragraph 33.

special categories of data and, therefore, that was not taking place or relevant to the herein Complaint and Inquiry.

Moreover, I expressed the view that it was clear from the Terms of Service that any sharing with affiliated companies formed part of the general “improvements” that are carried out pursuant to Article 6(1)(b) GDPR and so, in reality, any clear delineation between these two forms of processing was artificial. I also noted, in this regard, WhatsApp’s position that any “*sharing of WhatsApp user data to Meta Companies takes place on a controller to processor basis only, there does not need to be a distinct legal basis supporting it (or assessment of this issue in the Inquiry).*”⁴⁸

3.34 WhatsApp’s Terms of Service states that:

*“**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.”*

3.35 It further states that:

*“**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.”*

3.36 The Complainant however argues that such improvements and security features referenced in these terms, and any associated sharing of data with other Meta Companies (then Facebook Companies), is not necessary in order to deliver a messaging service, and that simply placing these terms in the contract does not make them necessary. Both of these statements may be true but, as noted in the Draft Decision, it does not follow that fulfilling these terms is not necessary in order to fulfil the specific contract with WhatsApp. To do that, to use the language of the EDPB, it is necessary to consider “*the nature of the service being offered to the data subject*”. In the Draft Decision, I expressed the view that WhatsApp’s improvement through utilising metrics gleaned from data, as

⁴⁸ WhatsApp submissions on Preliminary Draft, paragraph 7.9(B).

well as the contractual commitment to deal with abusive activity, marks out “*distinguishing characteristics*” (to use the language of the EDPB).⁴⁹ I further expressed the view that the WhatsApp service is clearly “*promoted [and] advertised*”,⁵⁰ via the Terms of Service as be one that provides both regular updates and improvements through use of data and one that has particular policies for dealing with abuse. I therefore expressed the view, in the Draft Decision, that a reasonable user would be well-informed that this is precisely the nature of the service being offered by WhatsApp and contained within the contract. WhatsApp expressed agreement with this position.⁵¹ I further indicated that this is true irrespective of any transparency deficiencies raised in the Complaint, including some found by the Commission in a previous Inquiry into WhatsApp’s Privacy Policy.

- 3.37 However, the position of the Complainant, and of the EDPB, seems to go so far as to say that processing will generally only be necessary for the performance of the contract if not carrying out the processing would make the performance of the contract impossible. Moreover, the position of the EDPB is that:

“The EDPB does not consider that Article 6(1)(b) would generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service. In most cases, a user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user.”⁵²

- 3.38 The EDPB has also opined that processing for fraud prevention is unlikely to be necessary to perform a contract.⁵⁶
- 3.39 The Guidelines, while not binding on the Commission, in my view clearly set out a very restrictive view on when processing should be deemed to be “necessary” for the performance of a contract, and explicitly refer to improvements to services as an example of processing that will usually not be necessary. It is notable that this is presented as a general rather than absolute rule, and refers to an “existing” service and the development of new functions. There is nothing contained in the Guidelines that would explicitly

⁴⁹ 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 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-badopted_after_public_consultation_en.pdf, paragraph 33.

⁵⁰ *Ibid.*

⁵¹ WhatsApp submissions on Preliminary Draft, paragraphs 7.14-7.15.

⁵² 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 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-badopted_after_public_consultation_en.pdf, paragraph 46. ⁵⁶ *Ibid.*, paragraph 47.

prohibit, in general, the processing of data that is necessary to fulfil a contractual term that commits to improving the functionality, efficiency, etc. of an existing service, as opposed to collecting data for the purpose of adding new features. Given the processing outlined in the Terms of Service relates to the former, I expressed the view, in the Draft Decision, that it falls outside of the scenario referred to by the EDPB. WhatsApp has expressed agreement with this point in its submissions on the Preliminary Draft.⁵³

3.40 In the Draft Decision, I expressed the view that the core area of dispute in applying Article 6(1)(b) GDPR on the facts was the question of whether the inclusion of service improvements and security, including through sharing data with another company, makes the processing of data conditional on the delivery of a contract, where that processing is not itself necessary to actually deliver the contract. The counter-argument is that these core elements of the specific service being offered are necessary to provide the WhatsApp service.

3.41 Applying the standards set out above to these particular circumstances, it seemed to me, when preparing the Draft Decision, that WhatsApp's model and the service being offered is explicitly one that includes improvements to an existing service, and a commitment to uphold certain standards relating to abuse, etc., that is common across all affiliated platforms. The EDPB has, of course, set out that processing cannot be rendered lawful by Article 6(1)(b) GDPR "*simply because processing is necessary for the controller's wider business model*".⁵⁴ In my view, the core of the service, however, as set out in the specific contract with the data subject, clearly includes these services. Moreover, there has been no suggestion that the utilisation of such data for these services is somehow a requirement that is specific to a commercial model, but rather is a term of a service being offered to users. When the surrounding principles are applied directly to the contract in question, I expressed the view, in the Preliminary Draft, that such processing is necessary to deliver the service being offered. WhatsApp has emphasised in its submissions on the Preliminary Draft that the processing in question can be distinguished from the EDPB Guidelines on this basis.⁵⁵

3.42 Further support for this particular view can be found in the answers to the specific questions posed in the EDPB Guidelines and set out at paragraph 3.36, above. The nature of the service being offered to WhatsApp users is set out in the Terms of Service, as I have already addressed. Moreover, a distinguishing feature of the WhatsApp service is that it regularly monitors its service in order to ensure it functions well (as distinct from the

⁵³ WhatsApp submissions on Preliminary Draft, paragraph 7.19.

⁵⁴ 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 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-adopted_after_public_consultation_en.pdf, paragraph 36.

⁵⁵ WhatsApp submissions on Preliminary Draft, paragraph 7.20.

EDPB's difficulty, in the Guidelines, with using data to bring about new services) and maintains certain security and abuse standards. The provision of this form of service is, in my view, part of the substance and fundamental object of the contract. As this information is both clearly set out and publicly available, I expressed the view, in the Draft Decision, that it would be difficult to argue that this is not part of the mutual expectations of a prospective user and of WhatsApp. I further expressed the view that it was clear that the service is advertised as being one that has these features, and so any reasonable user would expect and understand that this was part of the agreement, even if they would prefer the market would offer them better alternative choices. I was therefore satisfied that the answers to all of the questions proposed by the EDPB suggest that the Complainant's application of Article 6(1)(b) GDPR on the facts is inaccurate, and that nothing in the Guidelines prevent WhatsApp, in principle, from relying on Article 6(1)(b) GDPR for these purposes.

- 3.43 Finally I note that the Complainant has sought to rely on a Gallup poll, that suggests that the majority of users when agreeing to use Facebook (as opposed to WhatsApp) believed they were consenting to data processing rather than entering into a contract. The Complainant argues that it can be extrapolated that the situation in respect of WhatsApp is similar.⁵⁶ While no evidence for this has been presented, I was, in any event, not satisfied that such subjective impressions have any impact on whether a document is or is not a contract. Moreover, I was of the view, in the Draft Decision, that it certainly has no impact on the question of whether, in principle, a data controller may rely on a particular provision of Article 6 GDPR in order to legitimise particular forms of processing.
- 3.44 I have already pointed out my view that the Guidelines are non-binding. I was minded, nonetheless, in the Draft Decision, to agree with the arguments of both the Complainant and the EDPB in relation to the correct interpretation of Article 6(1)(b) GDPR. For the reasons set out above, my view was that nothing in the Complainant's submissions, the GDPR, the case law or the EDPB Guidelines suggest that the specific processing at issue, for the specific service being offered by WhatsApp, could not, in principle, be legitimised by Article 6(1)(b) GDPR.
- 3.45 While I accept that this assessment requires an element of reasoning in the abstract (in particular, when considering the mutual perspectives and expectations), I would add that the "core functions" assessment is more sensitive to the (potentially competing) rights of both parties, including WhatsApp's right to conduct a business pursuant to Article 16 of the Charter of Fundamental Rights and Freedoms (and freedom of contract generally). I am also of the view that it is not for an authority such as the Commission, tasked with the enforcement of data protection law, to make assessments as to what will or will not make

⁵⁶ Complainant submissions on Draft Inquiry Report, paragraph 3.3.1.

⁶¹ WhatsApp submissions on Preliminary Draft, Paragraph 7.16.

the performance of a contract possible or impossible. Instead, the general principles set out in the GDPR and explained by the EDPB in the Guidelines must be applied. These principles should be applied on a case-by-case basis, and in my view should be afforded more weight than generalised examples provided in the Guidelines, which are helpful and instructive but are by no means absolute or conclusive.

- 3.46 While WhatsApp has expressed agreement in general with the above analysis,⁵¹ it also argues that even if the Commission were to apply what it terms “the Impossibility Assessment” (which it nonetheless argues is the incorrect test), the processing would be permissible in principle. It submits that given the particular service being offered and advertised in a certain manner and the reasonable expectations of ordinary users, the processing associated with service improvements is in fact necessary, such that the performance of the contract would be rendered impossible if it was not carried out.⁵⁷
- 3.47 In the Draft Decision, I expressed the view that nothing precludes WhatsApp from relying on Article 6(1)(b) GDPR to deliver a service that includes the use of personal data for regular improvements and maintaining standards of security. Moreover, other provisions of the GDPR (such as transparency, which I consider at Issue 3, below) act to strictly regulate the manner in which this service is to be delivered, and the information that should be given to users.
- 3.48 Having analysed the submissions of the parties, the GDPR and the jurisprudence and Guidelines (with the caveats set out above), I found no basis, in the Draft Decision, for the contention that WhatsApp is precluded, in principle, from relying on Article 6(1)(b) GDPR for the purposes of legitimising the personal data processing activities involved in the provision of its service to users, including those considered herein. I expressed the view that nothing in the GDPR restricts or prohibits the use of these terms in the context of processing personal data *per se*. As has been set out earlier, and as set out by the Investigator, it is not for the Commission to rule on matters of contract law and contractual interpretation that extend beyond the remit of data protection law. The lawful basis under Article 6(1)(b) GDPR simply states that personal data may be processed where it is necessary for the performance of a contract. In other words and, as I have already set out in my analysis, the data may be processed if, without that processing, the contract would not be performed. I also expressed the view, in the Draft Decision, that this application conforms broadly to the interpretation of Article 6(1)(b) GDPR proposed by the Complainant and by the EDPB.
- 3.49 While I accept that, as a general rule, the EPDB considers that processing for the provision of new services, or the prevention of fraud, would not be necessary for the performance

⁵⁷ *Ibid*, paragraph 7.17.

of a contract for online services, in this particular case, having regard to the specific terms of the contract and the nature of the service provided and agreed upon by the parties, I concluded in the Draft Decision that WhatsApp may, in principle, rely on Article 6(1)(b) GDPR for the processing of users' data that is necessary for the provision of its service, including through the improvement of the existing service and the maintenance of security standards. As already noted above, the Complainant did not provide submissions on this or any issue in response to the Preliminary Draft.

- 3.50 I proposed to conclude, in the Draft Decision, that I was therefore satisfied that WhatsApp was, in principle, entitled to rely on Article 6(1)(b) GDPR for processing personal data on foot of the Complainant's acceptance of the Terms of Service. Having regard to the scope of the Complaint and this Inquiry, I added that this proposed conclusion was not to be construed as an indication

that all processing operations carried out on users' personal data were necessarily covered by Article 6(1)(b) GDPR.

- 3.51 Following the circulation of the Draft Decision to the supervisory authorities concerned, for the purpose of enabling them to express their views in accordance with Article 60(3) GDPR, objections to this aspect of matters were raised by the supervisory authorities of Germany, Finland, France, the Netherlands and Norway. Having considered the merits of those objections, the EDPB determined as follows:

90. As a preliminary remark, the EDPB notes, as observed by the NL SA, that the purposes are vague, especially the one on "safety and security", mentioned by WhatsApp IE in its Terms of Service. The EDPB understands from the short description provided under the relevant section of WhatsApp IE's Terms of Service that it refers to "misuse" of WhatsApp services, "harmful conduct", and activities that would violate WhatsApp IE's Terms of Service. In its Draft Decision, the IE SA considered that the Complainant did not identify particular processing operations with any degree of specificity, and that complaints should in general have a reasonable degree of specificity, and, hence addressed the issue of Article 6(1)(b) GDPR in principle. In doing so, the Draft Decision refers to various terms: "abusive activity" (which is referred to in WhatsApp IE's Terms of Service)⁶³, "fraud"⁶⁴ and "security" without further description⁶⁵ (which is referred to in WhatsApp IE's Terms of Service), which do not bring clarity and/or more specificity on this purpose. Based on these elements, and considering that WhatsApp IE's Terms of Service refer to another purpose of processing than the security carried out by technical and organisational measures in order to secure the processing of personal data, networks and services or processing to which WhatsApp IE is entitled or obliged under other legal provisions (e.g. technical and organisational measures applied to protect personal data, for instance as required under Article 32 GDPR⁶⁶), the EDPB is excluding "IT Security" from its assessment of the merits hereinafter. On a similar note, the EDPB highlights that when the purpose of the processing is "IT Security", for instance in the meaning of Article 32 GDPR, the purpose of the processing has to be clearly and specifically identified by the controller⁶⁷.

91. The EDPB considers that the objections found to be relevant and reasoned in this subsection⁶⁸ require an assessment of whether the Draft Decision needs to be changed insofar as it rejects the Complainant's claim that the GDPR does not permit WhatsApp IE's reliance on Article 6(1)(b) GDPR for the processing operations set out in its Terms of

⁶³ Draft Decision, paragraphs 4.36, 4.41, 4.42.

⁶⁴ Draft Decision, paragraphs 4.38 and 4.49.

⁶⁵ Draft Decision, paragraphs 4.40, 4.42, 4.47, 4.49.

⁶⁶ WhatsApp IE may also fall under legal duties to protect the security of its networks and services, as required by other laws. See for instance Article 40 of the European Electronic Communications Code established under Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018.

⁶⁷ See Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 16.

⁶⁸ Objections concerning the issue on the applicability of Article 6(1)(b) GDPR for purposes of service improvement and security features were raised by the DE SA, FI SA, FR SA, NL SA, and NO SA.

Service. When assessing the merits of the objections raised, the EDPB also takes into account WhatsApp IE's position on the objections and its submissions.

92. The CSAs seek in essence to establish whether Article 6(1)(b) GDPR could serve as a valid legal basis for the processing of personal data at issue, namely for service improvements and security features, in the specific case and to establish whether there is an infringement of Article 6(1) GDPR.
93. The CJEU has found that so far as concerns the principles relating to lawfulness of processing, Article 6 GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be considered lawful, processing must fall within one of the cases provided for in Article 6 GDPR⁶⁹ and it is the controller's obligation to provide and to be able to prove that the correct legal basis is applied for the respective processing.
94. The EDPB considers that there is sufficient information in the file for it to decide whether the IE SA needs to change its Draft Decision insofar as it rejects the Complainant's claim that the GDPR does not permit WhatsApp IE's reliance on Article 6(1)(b) GDPR to process personal data in the context of its offering of its Terms of Service.
95. As described above, in Section 4.3, the IE SA concludes in Finding 2 of its Draft Decision that the Complainant's case is not made out that the GDPR does not permit the reliance by WhatsApp IE on Article 6(1)(b) GDPR in the context of the latter offering its Terms of Service. Neither Article 6(1)(b) GDPR nor any other provision of the GDPR precludes WhatsApp IE from relying on Article 6(1)(b) GDPR as a legal basis to deliver a service, including the improvement of the existing service and the maintenance of security standards insofar as that forms a core part of the service⁷⁰. The IE SA considers that, having regard to the specific terms of the contract and the nature of the service provided and agreed upon by the parties, WhatsApp IE may in principle rely on Article 6(1)(b) GDPR as a legal basis of the processing of users' data necessary for the provision of its WhatsApp services, on foot of the Complainant's acceptance of the Terms of Service⁷¹. The IE SA considers that this information is clearly set out, publicly available and understandable by any reasonable user⁷². WhatsApp IE supports the IE SA's conclusion⁷³.
96. To assess the IE SA and WhatsApp IE's claims, the EDPB considers it necessary to recall the general objectives that the GDPR pursues, which must guide its interpretation, together with the wording of its provisions and its normative context⁷⁴.

⁶⁹ Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraphs 37 and 38.

⁷⁰ Draft Decision, paragraph 4.49.

⁷¹ Draft Decision, paragraph 4.50.

⁷² Draft Decision, paragraph 4.42.

⁷³ WhatsApp IE's Article 65 Submission, paragraphs 5.47.

⁷⁴ Judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20,), EU:C:2022:601, paragraph 121.

97. The GDPR develops the fundamental right to the protection of personal data found in Article 8(1) of the EU Charter and Article 16(1) of the Treaty on the Functioning of the EU, which constitute EU primary law⁷⁵. As the CJEU clarified, “an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law”⁷⁶. In view of rapid technological developments and increases in the scale of data collection and sharing, the GDPR creates a strong and more coherent data protection framework in the EU, backed by strong enforcement, and built on the principle that natural persons should have control over their own personal data⁷⁷. By ensuring a consistent, homogenous and equivalent high level of protection throughout the EU, the GDPR seeks to ensure the free movement of personal data within the EU⁷⁸. The GDPR acknowledges that the right to data protection needs to be balanced against other fundamental rights and freedoms, such as the freedom to conduct a business, in accordance with the principle of proportionality⁷⁹ and has these considerations integrated into its provisions. The GDPR, pursuant to EU primary law, treats personal data as a fundamental right inherent to data subjects and their dignity, and not as a commodity, they can trade away through a contract⁸⁰. The CJEU provided additional interpretative guidance by asserting that the fundamental rights of data subjects to privacy and the protection of their personal data override, as a rule, a controller’s economic interests⁸¹.
98. The principle of lawfulness under Article 5(1)(a) and Article 6 GDPR is one of the main safeguards to the protection of personal data. It follows a restrictive approach whereby a controller may only process the personal data of individuals if it is able to rely on one of the basis found in the exhaustive and restrictive lists of the cases in which the processing of data is lawful under Article 6 GDPR⁸².
99. The principle of lawfulness goes hand in hand with the principles of fairness and transparency in Article 5(1)(a) GDPR. The principle of fairness includes, *inter alia*, recognising the reasonable expectations of data subjects, considering possible adverse consequences a processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller⁸³.

⁷⁵ Recitals 1 and 2 GDPR.

⁷⁶ Judgment of 21 June 2022, *Ligue des droits humains v. Conseil des ministres*, C-817/19, EU:C:2022:491, paragraph 86; and judgment of 2 February 2021, *Consob*, C-481/19, EU:C:2021:84, paragraph 50 and the case-law cited.

⁷⁷ Article 1(1)(2) and recital 6 and 7 GDPR.

⁷⁸ Article 1(3) and recitals 9, 10 and 13 GDPR.

⁷⁹ Recital 4 GDPR.

⁸⁰ Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 54.

⁸¹ Judgment of 13 May 2014, *Google Spain SL*, C-131/12, EU:C:2014:317, paragraphs 97 and 99.

⁸² Judgment of 11 December 2019, *TK v Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraph 37.

⁸³ See, recital 39 GDPR and Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraphs 11 and 12.

100. The EDPB agrees with the IE SA and WhatsApp IE that there is no hierarchy between Article 6(1) legal bases⁸⁴. However, this does not mean that a controller, as WhatsApp IE in the present case, has absolute discretion to choose the legal basis that suits better its commercial interests. The controller may only rely on one of the legal bases established under Article 6 GDPR if it is appropriate for the processing in question⁸⁵. A specific legal basis will be appropriate insofar as the processing can meet its requirements set by the GDPR⁸⁶ and fulfil the objective of the GDPR to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. A legal basis will not be appropriate if its application to a specific processing defeats this practical effect “*effet utile*” pursued by the GDPR and its Article 5(1)(a) and Article 6 GDPR⁸⁷. These criteria stem from the content of the GDPR⁸⁸ and the interpretation favourable to the rights of data subjects to be given thereto described in paragraph 97 above.

101. The GDPR makes WhatsApp IE, as the controller for the processing at stake, directly responsible for complying with the GDPR’s principles, including the processing of data in a lawful, fair and transparent manner, and any obligations derived therefrom⁸⁹. This obligation applies even where the practical application of GDPR principles such as those of Article 5(1)(a) and Article (5)(2) GDPR are inconvenient or run counter to the commercial interests of WhatsApp IE. The controller is also obliged to be able to demonstrate that it meets these principles and any obligations derived therefrom, such as that it meets the specific conditions applicable to each legal basis⁹⁰. More specifically, this condition to be able to rely on Article 6(1)(b) GDPR as a legal basis to process the data subject’s data implies that a controller, in line with its accountability obligations under Article 5(2) GDPR, has to be able to demonstrate that (a) a contract exists and (b) the contract is valid pursuant to applicable national contract laws⁹¹.

⁸⁴ Draft Decision, paragraph 2.9, and WhatsApp IE’s Article 65 Submission, paragraph 8.34.

⁸⁵ As mentioned in Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 18, the identification of the appropriate lawful basis is tied to the principles of fairness and purpose limitation. It will be difficult for controllers to comply with these principles if they have not first clearly identified the purposes of the processing, or if the processing of personal data goes beyond what is necessary for the specified purposes. See also Section 5 below on the potential additional infringement of the principles of fairness, purpose limitation and data minimisation.

⁸⁶ Judgment of 11 December 2019, *TK v Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraph 37.

⁸⁷ Judgment of 18 December 2008, *Heinz Huber v. Bundesrepublik Deutschland*, C-524-06, EU:C:2008:724, paragraph 52 on the concept of necessity being interpreted in a manner that fully reflects the objective of Directive 95/46/EC. On the importance of considering the practical effect (“*effet utile*”) sought by EU law in its interpretation, see also for instance: judgment of 21 June 2022, *Ligue des droits humains v. Conseil des ministres*, C-817/19, EU:C:2022:491, paragraph 195; and judgment of 17 September 2002, *Muñoz and Superior Fruiticola*, C-253/00, EU:C:2002:497, paragraph 30.

⁸⁸ Article 1(1)(2) and (5) GDPR.

⁸⁹ Article 5(2) GDPR “Principle of accountability” of controllers; see also Opinion of the Advocate General of 20 September 2022, *Meta Platforms e.a.*, C-252/21, EU:C:2022:704, paragraph 52.

⁹⁰ Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 26.

⁹¹ EDPB Binding decision 2/2022 on the dispute arisen on the draft decision of the IE SA regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, adopted on 28 July 2022 (hereinafter “**EDPB Binding decision 2/2022**”), paragraph 84.

102. The EDPB agrees that supervisory authorities do not have, under the GDPR, a broad and general competence in contractual matters. However, the EDPB considers that the supervisory tasks, that the GDPR bestows on supervisory authorities, imply a limited competence to assess a contract's general validity insofar as this is relevant to the fulfilment of their tasks under the GDPR⁹². Otherwise, the supervisory authorities would see their monitoring and enforcement task under Article 57(1)(a) GDPR limited to actions, such as verifying whether the processing at stake is necessary for the performance of a contract (Article 6(1)(b) GDPR), and whether a contract with a processor under Article 28(3) GDPR and data importer under Article 46(2) GDPR includes appropriate safeguards pursuant to the GDPR.

103. The DE SA and NL SA⁹³ argue that the validity of the contract for the WhatsApp services between the latter and the Complainant is questionable given the serious transparency issues in relation to the legal basis relied on⁹⁴. In contract law, as a general rule, both parties must be aware of the substance of the contract and of the obligations of both parties to the contract in order to willingly enter into such contract.

104. Notwithstanding the possible invalidity of the contract, the EDPB refers to its previous interpretative guidance on this matter⁹⁵ to provide below its analysis on whether the processing for the purposes of service improvement and security features⁹⁶ is objectively necessary for WhatsApp IE to provide its services to users based on its Terms of Service and the nature of the services.

105. The EDPB recalls⁹⁷ that for the assessment of necessity under Article 6(1)(b) GDPR, *"[i]t is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance"*⁹⁸. As the EDPB has previously stated, regard should be given to the particular aim, purpose, or objective of the service and, for applicability of Article 6(1)(b) GDPR, it is required that the processing is objectively necessary for a purpose and integral to the delivery of that contractual service to the data subject⁹⁹.

106. Moreover, the EDPB notes that the controller should be able to justify the necessity of its processing by reference to the fundamental and mutually understood contractual

⁹² EDPB Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraphs 9 and 13.

⁹³ DE SA's Objection, p.3 ; NL SA's Objection, paragraph 10.

⁹⁴ Draft Decision, paragraph 5.9.

⁹⁵ Guidelines 2/2019 on Article 6(1)(b) GDPR.

⁹⁶ For the term security, see paragraph 90 of this binding decision.

⁹⁷ EDPB Binding decision 2/2022, paragraph 89.

⁹⁸ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 Directive 95/46/EC, WP 217, adopted on 9 April 2014 (hereinafter, "**WP29 Opinion 06/2014 on the notion of legitimate interests**"), p. 17.

⁹⁹ Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 30.

purpose. This depends not only on the controller's perspective, but also on a reasonable data subject's perspective when entering into the contract ¹⁰⁰.

107. The IE SA accepts *"that, as a general rule, the EPDB considers that processing for the provision of new services [...] would not be necessary for the performance of a contract for online services"*¹⁰¹. However, the IE SA considers that in this particular case, having regard to the specific terms of the contract and the nature of the services provided and agreed upon by the parties, WhatsApp IE may in principle rely on Article 6(1)(b) GDPR to process the user's data necessary for the provision of its service, including through the improvement of the existing service and the maintenance of security standards.

108. In particular, the IE SA views service improvement to an existing service and *"a commitment to uphold certain standards relating to abuse, etc."* as a *"core"* element of the contract between WhatsApp IE and the users¹⁰². In support of this consideration, the IE SA refers to the information provided in the WhatsApp Terms of Service under the headings: *"Ways To Improve Our Services."* and *"Safety And Security."*¹⁰³ The IE SA considers that it is clear that the WhatsApp services are advertised (and widely understood) as ones that requires updates and improvement and so, that any reasonable user would *"be well-informed that this is precisely the nature of the service being offered by WhatsApp and contained within the contract"*¹⁰⁴.

109. The EDPB is of the opinion that WhatsApp IE is under the legal duty to assess whether the processing of all its users data is necessary for the purpose of service improvements or if there are alternative, less intrusive ways to pursue this purpose (e.g. instead of relying on all users' data for the purpose of service improvements, rely on a pool of users, who voluntarily agreed, by providing consent, to the processing of their personal data for this purpose).

110. On this issue, the EDPB recalls that the concept of necessity has its own independent meaning under EU law. It must be interpreted in a manner that fully reflects the objective pursued by an EU instrument, in this case, the GDPR¹⁰⁵. Accordingly, the concept of necessity under Article 6(1)(b) GDPR cannot be interpreted in a way that undermines this provision and the GDPR's general objective of protecting the right to the protection of personal data¹⁰⁶ or contradicts Article 8 of the EU Charter. On the processing of data in the WhatsApp services, Advocate General Rantos supports a strict interpretation of

¹⁰⁰ EDPB Binding decision 2/2022, paragraph 90.

¹⁰¹ Draft Decision, paragraph 4.49.

¹⁰² Draft Decision, paragraph 4.41.

¹⁰³ Draft Decision, paragraphs 4.34 and 4.35.

¹⁰⁴ Draft Decision, paragraph 4.36.

¹⁰⁵ See paragraphs 103-105 above on the principles guiding the interpretation of the GDPR and its provisions. The CJEU also stated in *Huber* that *"what is at issue is a concept [necessity] which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that Directive, [Directive 95/46], as laid down in Article 1(1) thereof"*. Judgment of 18 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, C-524/06, EU:C:2008:724, paragraph 52.

¹⁰⁶ Article 1(2) GDPR.

Article 6(1)(b) GDPR among other legal basis, particularly to avoid any circumvention of the requirement for consent¹⁰⁷.

111. The EDPB finds that an average user cannot fully grasp what is meant by processing for service improvement and security features, be aware of its consequences and impact on their rights to privacy and data protection, and reasonably expect it solely based on WhatsApp IE's Terms of Service. Advocate General Rantos expresses similar doubts where he states, in relation to Facebook behavioural advertising practices, "*According to the case-law of the Court of Justice, the processing must be objectively necessary for the performance of the contract in the sense that there must be no realistic, less intrusive alternatives, taking into account the reasonable expectations of the data subject. It also concerns the fact that, where the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of Article 6(1)(b) of the GDPR should be assessed in the context of each of those services separately*"¹⁰⁸ and adds in a footnote that "*Moreover, although merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b) of the GDPR, processing may be objectively necessary even if not specifically mentioned in the contract, without prejudice to the controller's transparency obligations*"¹⁰⁹.

112. The EDPB provides in its guidance¹¹⁰ assessing what is "necessary" involves a combined, fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal". If there are realistic, less intrusive alternatives, the processing is not "necessary". Article 6(1)(b) GDPR does not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject, even if it is necessary for the controller's other business purposes. While the possibility of improvements of services may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user¹¹¹.

113. When analysing the performance of a contract as a legal basis, the necessity requirement has to be interpreted strictly. As stated earlier by the Article 29 Working Party (hereinafter "WP29")¹¹², this "*provision must be interpreted strictly and does not*

¹⁰⁷ Opinion of the Advocate General of 20 September 2022, *Meta Platforms e.a.*, C-252/21, EU:C:2022:704, paragraph § 51. The EDPB refers to the Advocate General's Opinion in its Binding Decision as an authoritative source of interpretation to underline the EDPB's reasoning on the processing of data in the Facebook service, without prejudice to the case-law that the CJEU may create with its future judgments on Cases C-252/21 and C- 446/21.

¹⁰⁸ Opinion of the Advocate General of 20 September 2022, *Meta Platforms e.a.*, C-252/21, EU:C:2022:704, paragraph 54.

¹⁰⁹ *Ibid*, footnote 165.

¹¹⁰ Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 25.

¹¹¹ Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 49.

¹¹² The WP 29 - the predecessor of the EDPB - was established under Article 29 of 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 ("Directive 95/46/EC") and had a role, *inter alia*, to contribute to uniform application of national measures adopted under the Directive. Many of substantive principles and provisions of

cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller”¹¹³.

114. Concerning the processing of service improvement, the EDPB finds that a reasonable user cannot expect that their personal data is being processed for service improvement simply because WhatsApp IE briefly refers to this processing in its Terms of Service (which both WhatsApp IE and the IE SA consider as constituting the entirety of the contract), or because of the argument that *“on the basis of the cont[r]act and wider circumstances, that a reasonable user would have had sufficient understanding that the service included the use of metrics for improvement”* to which the IE SA refers¹¹⁴.

115. In addition, the IE SA already decided¹¹⁵ that WhatsApp IE infringed its transparency obligations under Article 5(1)(a), Article 12(1) and Article 13(1)(c) GDPR by not clearly informing the Complainant and other users of the WhatsApp IE services’ specific processing operations, the personal data processed in them, the specific purposes they serve, and the legal basis on which each of the processing operations relies, as the IE SA concludes in its Draft Decision¹¹⁶. The EDPB considers that this fundamental failure of WhatsApp IE to comply with its transparency obligations contradicts the IE SA’s finding¹¹⁷ that WhatsApp IE’s users could reasonably expect service improvement and security features as being necessary for the performance of their contract.

116. As regards security, the lack of clarity of the Terms of Service makes it even hard to understand what are the different purposes pursued and processing carried out ¹¹⁸.

117. The EDPB recalls that *“controllers should make sure to avoid any confusion as to what the applicable legal basis is”* and that 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”*, because *“[d]epending 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”¹¹⁹*. Article 6(1)(b) GDPR requires the existence of a contract, its validity, and the processing being necessary to perform it. These conditions cannot be met where one of the parties (in this case a data subject) is not provided with sufficient information to know that they are signing a contract, the processing of personal data that it involves, for which specific purposes and on which legal basis, and how this processing is necessary to perform the services delivered. For the purposes of service improvement and security features, WhatsApp IE has not relied on any other legal basis to process personal data. These transparency

the GDPR already existed in the Directive 95/46/EC, such as the one at stake in this Binding decision, thus WP29 guidance in this respect is relevant for the interpretation of the GDPR.

¹¹³ WP29 Opinion06/2014 on the notion of legitimate interests, p. 16.

¹¹⁴ Composite Response, paragraph 59.

¹¹⁵ Draft Decision, paragraph 5.9.

¹¹⁶ Draft Decision, paragraph 5.9 and Finding 3.

¹¹⁷ Draft Decision, paragraph 4.42.

¹¹⁸ For the meaning of the term “security”, see paragraph 90 above.

¹¹⁹ EDPB Binding Decision01/2021, paragraph 214, and Guidelines 2/2019 on Article 6(1)(b) GDPR, paragraph 20.

requirements are not only an additional and separate obligation, but also an indispensable and constitutive part of the legal basis.

118. Given that the main purpose for which a user uses the WhatsApp services is to communicate with others, and that WhatsApp IE conditions their use to the user's acceptance of a contract and the service improvement and security¹²⁰ features they include, the EDPB cannot see how a user would have the possibility of opting out of a particular processing which is part of the contract. Thus, WhatsApp IE is accountable to prove that the legal basis applied for the processing at hand is valid and the failure to demonstrate this proves that Article 6(1) GDPR is not the applicable legal basis.

119. The EDPB agrees with the DE SA, FI SA, FR SA, NL SA and NO SA¹²¹ that there is a risk that the Draft Decision's failure to establish WhatsApp IE's infringement of Article 6(1)(b) GDPR, pursuant to its interpretation by the IE SA, nullifies this provision and makes theoretically lawful any collection and reuse of personal data in connection with the performance of a contract with a data subject. WhatsApp IE currently leaves the Complainant and other users of the WhatsApp services with a "take it or leave it" choice. They may either contract away their right to freely determine the processing of their personal data and submit to its processing for service improvements or security features, which they can neither expect, nor fully understand based on the insufficient information WhatsApp IE provides to them. Alternatively, they may decline accepting WhatsApp IE's Terms of Service and thus be excluded from a service that enables them to communicate with millions of users.

120. This precedent could encourage other economic operators to use the contractual performance legal basis of Article 6(1)(b) GDPR for all their processing of personal data. There would be the risk that some controllers argue some connection between the processing of the personal data of their consumers and the contract to collect, retain and process as much personal data from their users as possible and advance their economic interests at the expense of the safeguards for data subjects. Some of the safeguards from which data subjects would be deprived due to an inappropriate use of Article 6(1)(b) GDPR as legal basis, instead of others such as consent under Article 6(1)(a) GDPR and legitimate interest under Article 6(1)(f) GDPR, are the possibility to specifically consent to certain processing operations and not to others and to the further processing of their personal data (Article 6(4) GDPR); their freedom to withdraw consent (Article 7 GDPR); their right to be forgotten (Article 17 GDPR); and the balancing exercise of the legitimate interests of the controller against their interests or fundamental rights and freedoms (Article 6(1)(f) GDPR).

¹²⁰ For the meaning of the term "security", see paragraph 90 above.

¹²¹ DE SA's Objections – p. 6, paragraph 2 and p. 8, paragraph 1; FI SA's Objections – p. 7, paragraphs 32 and 33; FR SA's Objections – paragraph 14; NL SA's Objections – paragraphs 8 and 28; NO SA's Objections – p. 4, paragraph 3.

121. The EDPB thus concurs with the objections of the DE SA, FI SA, FR SA, NL SA and NO SA¹²² to Finding 2 of the Draft Decision in that the processing for the purposes of service improvements and security¹²³ features performed by WhatsApp IE are objectively not necessary for the performance of WhatsApp IE's alleged contract with its users and are not an essential or core element of such contract.

122. In conclusion, the EDPB decides that WhatsApp IE has inappropriately relied on Article 6(1)(b) GDPR to process the Complainant's personal data for the purpose of service improvement and security¹²⁴ features in the context of its Terms of Service and therefore lacks a legal basis to process these data. The EDPB was not required to examine whether data processing for such purposes could be based on other legal bases because the controller relied solely on Article 6 (1) (b) GDPR. WhatsApp IE has consequently infringed Article 6(1) GDPR by unlawfully processing personal data. The EDPB instructs the IE SA to alter its Finding 2 of its Draft Decision which concludes that WhatsApp IE may rely on Article 6(1)(b) GDPR in the context of its offering of Terms of Service and to include an infringement of Article 6(1) GDPR based on the shortcomings that the EDPB has identified.

3.52 On the basis of the above, and as directed by the EDPB further to the Article 65 Decision, I find that WhatsApp was not entitled to rely on Article 6(1)(b) GDPR to process the Complainant's personal data for the purpose of service improvement and security in the context of the WhatsApp Terms of Service.

Finding 2:

I find that WhatsApp was not entitled to rely on Article 6(1)(b) GDPR to process the Complainant's personal data for the purpose of service improvement and security in the context of the WhatsApp Terms of Service.

4 ISSUE 3 – WHETHER WHATSAPP PROVIDED THE REQUISITE INFORMATION ON THE LEGAL BASIS FOR PROCESSING ON FOOT OF ARTICLE 6(1)(B) GDPR AND WHETHER IT DID SO IN A TRANSPARENT MANNER

4.1 Processing of personal data, including transparency requirements of the GDPR, are governed by the overarching principles set out in Article 5 GDPR, which provides that:

"1. Personal data shall be:

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

¹²² DE SA's Objections – p. 5, paragraphs 3 and 4; ; FI SA's Objections – p. 6, paragraph 24; FR SA's Objections – p. 7, paragraph 38 ; NL SA's Objections – paragraph 26; NO SA's Objections - p. 8.

¹²³ For the meaning of the term "security", see paragraph 90 above.

¹²⁴ For the meaning of the term "security", see paragraph 90 above.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

4.2 Recital 58 of the GDPR, which serves as an aid to interpretation, states:

"The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.

Such information could be provided in electronic form, for example, when addressed to the public, through a website.

This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and

understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.

Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.”

4.3 Article 12(1) GDPR provides for the general manner in which information required by the transparency provisions of the GDPR should be set out:

“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. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.”

4.4 Article 13 GDPR enumerates specific categories of information that must be provided to data subjects by data controllers in order to comply with transparency obligations:

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

- (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.

2. *In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:*

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

(b) 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;

(c) 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;

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

(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;

(f) 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.

3. *Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.*

4. *Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information."*

4.5 In its Transparency Guidelines, which have been adopted by the EDPB, the Article 29 Working Party found that:

“A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used.”⁵⁸

4.6 In the Complaint, the Complainant alleged that WhatsApp’s updated Terms of Service and the hyperlinked Data Policy, together with the mode of acceptance (namely, clicking an “accept” button) on the Terms of Service, created the conditions which led to the belief *“that all these processing operations”* were based on consent under 6(1)(a) GDPR.⁵⁹ The Investigator therefore examined whether it could be alleged that the Complainant was led to believe this was the case.

4.7 The Complainant argued that there was a lack of clarity in respect of the data processing which was carried out on foot of the “forced consent” to the Terms of Service. Indeed, the Complaint states that *“[e]ven if a trained lawyer reads all the text that the controller provides, he/she can only guess what data is processed, for which exact purpose and on which legal basis. This is inherently non-transparent and unfair within the meaning of Articles 5(1)(a) and 13(c).”*⁶⁰ Furthermore, the Complainant argued that:

“The controller has in fact relied on a number of legal grounds under Article 6(1) of the GDPR, but has given the data subject the impression, that he solely relies on consent, by requesting the data subject to agree to the privacy policy (see above). Asking for consent to a processing operation, when the controller relies in fact on another legal basis is fundamentally unfair, misleading and non-transparent within the meaning of Article 5(1)(a) of the GDPR...”

4.8 Therefore, and in accordance with my determination concerning the scope of the Complaint, as set out in the Draft Decision, I found that there was an inherent allegation in the Complaint that the legal basis relied on by WhatsApp for processing personal data in accordance with the acceptance of the Terms of Service is unclear. Article 5(1)(a) GDPR sets out the requirement that, at a general level, personal data must be processed in a transparent manner. More specific transparency requirements are contained in Articles 12 and 13 GDPR. In particular, Article 13(1)(c) GDPR requires that *“the purposes of the processing for*

⁵⁸ Article 29 Working Party Guidelines on transparency under Regulation 2016/679, page 7, paragraph 10, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

⁵⁹ Complaint, page 2.

⁶⁰ *Ibid.* paragraph 2.3.1.

which the personal data are intended as well as the legal basis for processing” must be made clear to a user. Article 12(1) GDPR states that the information that is required to be provided pursuant to Article 13 GDPR must be provided in a clear and transparent manner. Article 13 GDPR therefore prescribes the information which must be provided to the data subject whereas Article 12(1) GDPR sets out the way in which this information should be provided.

- 4.9 The Commission previously concluded an own-volition inquiry pursuant to Section 110 of the 2018 Act, and made a decision under Section 111 of the 2018 Act, in relation to the extent to which WhatsApp’s Privacy Policy achieved compliance with the GDPR’s transparency framework (“the **WhatsApp Transparency Decision**”). This included an assessment of compliance with these provisions of the GDPR in the context of processing carried out pursuant to Article 6(1)(b) GDPR. This decision made findings to the effect that the transparency provisions were infringed, including in relation to the information that WhatsApp was required to provide, pursuant to Articles 12(1) and 13(1)(c) GDPR, concerning any processing carried out pursuant to Article 6(1)(b) GDPR. The decision included the exercise of a number of corrective powers, including an administrative fine and an order requiring WhatsApp to bring the Privacy Policy into compliance. In circumstances where the issues raised by the transparency aspect of the Complaint have already, by way of the WhatsApp Transparency Decision, been examined and determined by the Commission, it is not necessary for me to carry out any further examination in relation to the same subject-matter in the context of this Inquiry. I note that the views expressed by the Complainant and her representative, in respect of this particular aspect of the Complaint, are consistent with the outcome of the corresponding part of the WhatsApp Transparency Decision. On this basis, it is clear that the Complainant has identified infringements of the GDPR, and I therefore uphold that aspect of the Complaint.
- 4.10 As noted above, a number of corrective powers were exercised against WhatsApp pursuant to the WhatsApp Transparency Decision, which took into account every impacted data subject in the EEA, including the Complainant. I further note, in this regard, that WhatsApp has already taken the action required to achieve compliance with the order to bring processing into compliance that was made further to the WhatsApp Transparency Decision. In these circumstances, I do not consider it appropriate, proportionate or necessary to exercise further corrective powers, in response to this particular finding of infringement.

Outcome re: Issue 3:

In relation to compliance with Articles 12(1) and 13(1)(c) GDPR for processing carried out on foot of Article 6(1)(b) GDPR, the Commission has already found in a previous inquiry that WhatsApp has infringed the GDPR in this regard. On the basis that the Complainant has identified infringements of the GDPR, this aspect of the Complaint is upheld.

5 ADDITIONAL ISSUE: WHETHER WHATSAPP INFRINGED THE ARTICLE 5(1)(A) PRINCIPLE OF FAIRNESS

5.1 During the course of the Article 60 consultation period, the Italian supervisory authority raised an objection to the Draft Decision, the purpose of which was to require the amendment of the Draft

Decision to include a new finding of infringement of the Article 5(1)(a) principle of fairness. The Commission decided not to follow the objection in circumstances where compliance with the Article 5(1)(a) principle of fairness was not examined during the course of this inquiry and, consequently, WhatsApp was never afforded the opportunity to be heard in response to a particularised allegation of wrongdoing, as required by Irish and EU law. Accordingly the Commission referred the objection to the EDPB for determination pursuant to Article 65(1)(a) GDPR. Having considered the matter, the EDPB determined as follows:

142. At first, the EDPB notes that the concept of fairness 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 of personal data. An important aspect of the principle of fairness under Article 5(1) GDPR, which is linked to recital 39, is that data subjects should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data have been used¹²⁸.

143. Fairness is an overarching principle, which requires that personal data shall not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectification) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processing)¹²⁹.

144. The principles of fair and transparent processing require that the data subject shall be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling¹³⁰.

145. The EDPB underlines that the principles of fairness, lawfulness and transparency, all three enshrined in Article 5(1)(a) GDPR, are three distinct but intrinsically linked and interdependent principles that every controller should respect when processing personal data. The link between these principles is evident from a number of GDPR provisions: recitals 39 and 42, Article 6(2) and Article 6(3)(b) GDPR refer to lawful and fair processing, while recitals 60 and 71 GDPR, as well as Article 13(2), Article 14(2) and Article 40(2)(a) GDPR refer to fair and transparent processing.

¹²⁸ WP29 Guidelines on transparency under Regulation 2016/679, paragraph 10.

¹²⁹ EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2, Adopted on 20 October 2020, hereinafter “**Guidelines on Data Protection by Design and by Default**”.

¹³⁰ Recital 60 GDPR.

146. The IT SA states that *“the infringement of Article 5(1)(a) GDPR should be found by the LSA in the case at hand by having also regard to the more general fairness principle, which entails separate requirements from those relating specifically to transparency.”*¹³¹

147. There is no dispute that in its Decision on WhatsApp IE’s Transparency, the IE SA found a breach of the transparency principle, but the EDPB considers that the principle of fairness has an independent meaning and stresses that an assessment of WhatsApp IE’s compliance with the principle of transparency does not automatically rule out the need for an assessment of WhatsApp IE’s compliance with the principle of fairness too.

148. The EDPB recalls that, in data protection law, the concept of fairness stems from the EU Charter¹³². The EDPB has already provided some elements as to the meaning and effect of the principle of fairness in the context of processing personal data. For example, the EDPB has previously opined in its Guidelines on Data Protection by Design and by Default that *“Fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject”*¹³³. Among the key fairness elements that controllers should consider in this regard, the EDPB mentions autonomy of the data subjects, data subjects’ expectation, power balance, avoidance of deception, ethical and truthful processing¹³⁴. These elements are particularly relevant in the case at hand. The principle of fairness under Article 5(1)(a) GDPR underpins the entire data protection framework and seeks to address power asymmetries between controllers and data subjects in order to cancel out the negative effects of such asymmetries and ensure the effective exercise of data subjects’ rights.

149. The EDPB has previously explained that *“the principle of fairness includes, inter alia, recognising the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller”*¹³⁵. The EDPB recalls that a fair balance must be struck between, on the one hand, the commercial interests of controllers and, on the other hand, the rights and expectations of data subjects under the GDPR¹³⁶. A key aspect of compliance with the principle of fairness under Article 5(1)(a) GDPR refers to pursuing “power balance” as a “key objective

¹³¹ IT SA’s Objection, paragraph 3, p. 9.

¹³² Article 8 of the EU Charter states as follows: *“1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”* (emphasis added).

¹³³ EDPB 4/2019 Guidelines on Article 25, Data Protection by Design and by Default, version 2, adopted on 20 October 2022, (hereinafter “**Guidelines on Data Protection by Design and by Default**”) paragraph 69.

¹³⁴ Guidelines on Data Protection by Design and by Default, paragraph 70.

¹³⁵ Guidelines on Article 65(1)(a), paragraph 12.

¹³⁶ On the balance between the different interests at stake see for example: Judgment of 12 December 2013, X, C-486/12, EU:C:2013:836; Judgment of 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07, EU:C:2009:293; Judgment of 9 November 2010 in joined cases, *Volker und Markus Schecke GbR*, C-92/09, and *Hartmut Eifert*, C-93/09, *v Land Hessen*, EU:C:2010:662.

*of the controller-data subject relationship*¹³⁷, especially in the context of online services provided without monetary payment, where users are often not aware of the ways and extent to which their personal data is being processed¹³⁸. Consequently, if data subjects are not enabled to determine what is done with their personal data, this is in contrast with the element of “autonomy” of data subjects as to the control of the processing of their personal data¹³⁹.

150. Considering the constantly increasing economic value of personal data in the digital environment, it is particularly important to ensure that data subjects are protected from any form of abuse and deception, intentional or not, which would result in the unjustified loss of control over their personal data. Compliance by providers of online services acting as controllers with all three of the cumulative requirements under Article 5(1)(a) GDPR, taking into account the particular service that is being provided and the characteristics of their users, serves as a shield from the danger of abuse and deception, especially in situations of power asymmetries. Therefore, the EDPB disagrees with the IE SA’s finding that assessing WhatsApp IE’s compliance with the principle of fairness “*would therefore not only represent a significant departure from the scope of inquiry, as formulated, but it would also risk breaching the controller’s right to a fair procedure, as regards any matter which was never put to the complainant during the course of inquiry.*”¹⁴⁰ In addition, it is important to note that WhatsApp IE has been heard on the objections and therefore submitted written submissions on this matter¹⁴¹.

151. The EDPB has previously emphasised that the identification of the appropriate lawful basis is tied to the principles of fairness and purpose limitation¹⁴². In this regard, the IT SA rightly observes that while finding a breach of transparency relates to the way in which information has been provided to users via the terms of service and the Privacy Policy, compliance with the principle of fairness also relates to ‘*how the controller addressed the lawfulness of the processing activities in connection with its calling and messaging service*’¹⁴³. Thus, the EDPB considers that an assessment of compliance by WhatsApp IE with the principle of fairness requires also an assessment of the consequences that the choice and presentation of the legal basis entail for the WhatsApp services’ users. In addition, that assessment cannot be made in the abstract, but has to take into account the specificities of the particular messaging service and of the processing of personal data carried out, namely for purposes related to improvements of the messaging service¹⁴⁴.

¹³⁷ Guidelines on Data Protection by Design and by Default, paragraph 70.

¹³⁸ On “online services”, see Guidelines 1/2019 on Article 6(1)(b) GDPR, paragraphs 3-5.

¹³⁹ Guidelines on Data Protection by Design and by Default, paragraph 70. According to this element of fairness, “*data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing*”.

¹⁴⁰ Composite Response, paragraph 30.

¹⁴¹ WhatsApp IE’s Article 65 Submissions, Category 1f: “*The [Commission] should also make findings that WhatsApp Ireland infringed the fairness principle under Article 5(1)(a) GDPR/ lawfulness principle under Article 5(1)(a) GDPR*”, p. 31.

¹⁴² Guidelines 1/2019 on Article 6(1)(b) GDPR, paragraph 1.

¹⁴³ IT SA’s Objection, p. 9.

¹⁴⁴ Draft Decision, paragraph 4.40.

152. The EDPB notes that in this particular case, the Complainant was forced to consent to the Terms of Service and the Privacy Policy¹⁴⁵ and this clearly impacts the reasonable expectations of WhatsApp IE's users by confusing them on whether clicking the "Accept" button results in giving their consent to the processing of their personal data. The EDPB notes in this regard that one of the elements of compliance with the principle of fairness is avoiding deception (i.e. providing information *"in an objective and neutral way, avoiding any deceptive or manipulative language or design"*¹⁴⁶).

153. As the IE SA itself notes, the Complainant argues that WhatsApp IE relied on "forced consent" for the processing simply because it did in fact believe that the controller was relying on the legal basis of consent for that processing¹⁴⁷. The Complainant presents the screenshot, aiming to demonstrate that, *"the data subject was presented with an easy click to quickly consent, and to return to the service."*¹⁴⁸ The EDPB keeps in mind that in the complaint, this was explained in the context of arguing that consent was forced. Therefore, the EDPB shares the IT SA's concern that WhatsApp IE misrepresented the legal basis of the processing and that WhatsApp IE's users are left "in the dark" as to the possible connections between the purposes sought, the applicable legal basis and the relevant processing activities¹⁴⁹. This being said, the EDPB considers that the processing by WhatsApp IE cannot be regarded as ethical and truthful¹⁵⁰ because it is confusing with regard to the type of data processed, the legal basis used and the purposes of the processing, which ultimately restricts the WhatsApp IE's users' possibility to exercise their data subjects' rights.

154. Considering the seriousness of WhatsApp IE's misrepresentation on the legal basis relied on identified in the current Binding decision¹⁵¹, the EDPB agrees with the IT SA that WhatsApp IE has presented its service to its users in a misleading manner¹⁵², which adversely affects their control over the processing of their personal data and the exercise of their data subjects' rights.

155. This is all the more supported by the fact that the circumstances of the present case as demonstrated above¹⁵³ and the infringement of Article 6(1)(b) GDPR¹⁵⁴ further intensify the imbalanced nature of the relationship between WhatsApp IE and its users brought up by the IT SA's objection.

¹⁴⁵ See paragraph 3 above.

¹⁴⁶ Guidelines on Data Protection by Design and by Default, paragraph 70.

¹⁴⁷ Draft Decision, paragraph 5.7.

¹⁴⁸ Complaint, p. 5.

¹⁴⁹ IT SA's Objection, p. 9.

¹⁵⁰ Guidelines on Data Protection by Design and by Default, paragraph 70, where the EDPB explains that "ethical" means that *"The controller should see the processing's wider impact on individuals' rights and dignity"* and "truthful" means that *"The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects"*.

¹⁵¹ See, paragraph 117 above.

¹⁵² IT SA Objection, page 9.

¹⁵³ Draft Decision, paragraphs 148-153.

¹⁵⁴ Draft Decision, paragraphs 117 and 122.

156. The combination of factors, such as the unbalanced relationship between WhatsApp IE and its users, combined with the “take it or leave it” situation that they are facing due to the lack of alternative services in the market and the lack of options allowing them to adjust or opt out from a particular processing under their contract with WhatsApp IE, systematically disadvantages them, limits their control over the processing of their personal data and undermines the exercise of their rights under Chapter III GDPR.

157. Therefore, the EDPB instructs the IE SA to include a finding of an infringement of the principle of fairness under Article 5(1)(a) GDPR by WhatsApp IE and to adopt the appropriate corrective measures, by addressing, but without being limited to, the question of an administrative fine for this infringement as provided for in Section 8 of this Binding decision.

5.2 Accordingly, and as directed by the EDPB further to the Article 65 Decision, I find that WhatsApp has infringed the principle of fairness pursuant to Article 5(1)(a) GDPR.

Finding 4:
I find that WhatsApp has infringed the principle of fairness pursuant to Article 5(1)(a) GDPR.

6 **SUMMARY OF FINDINGS/OUTCOME**

ISSUE	FINDING/OUTCOME
Reliance on Article 6(1)(b) GDPR	I find that WhatsApp infringed Article 6(1) GDPR when it relied on Article 6(1)(b) GDPR to process the Complainant’s personal data for the purpose of service improvement and security in the context of its offering of Terms of Service.
Whether WhatsApp failed to provide necessary information regarding its legal basis for processing pursuant to acceptance of the Terms of Service and whether the information set out was set out in a transparent manner.	The Commission has found infringements in this regard in a previous inquiry (and exercised corrective powers in response).
As raised by the Italian SA by way of its objection, whether WhatsApp infringed the Article 5(1)(a) principle of fairness in the context of its approach to the provision of information as part of the presentation of its Terms of Service to the Complainant.	As directed by the EDPB pursuant to the Article 65 Decision, I find that WhatsApp has infringed the Article 5(1)(a) principle of fairness.

7 DECISION ON CORRECTIVE POWERS

- 7.1 In the Draft Decision, I proposed to conclude findings of infringement of Articles 12(1) and 13(1)(c) GDPR. As already noted, further to the assessment of Issue 3, above, these proposed findings overlapped with those that were already found to have occurred in the WhatsApp Transparency Decision. As further noted, a number of corrective powers were exercised against WhatsApp pursuant to the WhatsApp Transparency Decision, which took into account every impacted data subject in the EU/EEA, including the Complainant. I further note that WhatsApp has already taken the action required to achieve compliance with the order to bring processing into compliance that was made further to the WhatsApp Transparency Decision such that the identified transparency deficits have since been rectified. In these circumstances, the exercise of further corrective powers, in response to the upholding of the transparency element of the Complaint, could not be considered to be appropriate, proportionate or necessary.
- 7.2 As a consequence, however, of the infringements of Article 6(1) and the Article 5(1)(a) principle of fairness that were established by the EDPB in the Article 65 Decision, the EDPB further directed the Commission to address those infringements by way of the exercise of corrective powers, namely the making of an order to bring processing into compliance and the imposition of an administrative fine.

8 ORDER TO BRING PROCESSING INTO COMPLIANCE

- 8.1 The requirement to make an order to bring processing into compliance, in connection with the Article 6(1) infringement, arose from an objection that was raised by the Finnish supervisory authority during the course of the Article 60 GDPR consultation period. That objection required the Commission to both establish a finding of infringement of Article 6(1) GDPR (which was determined by the EDPB, as already detailed above) and, as a consequence of that finding, to make an order requiring WhatsApp to bring its processing into compliance. Considering this, second, limb of the Finnish objection, the EDPB determined as follows:

“269. The EDPB agrees with the FI SA that “the infringement cannot be consider as minor”. The EDPB reiterates that lawfulness of processing is one of the fundamental pillars of the data protection law and considers that processing of personal data without an appropriate legal basis is a clear and serious violation of the data subjects’ fundamental right to data protection. In addition, the infringement in the present case concerns a high number of data subjects and a large amount of personal data.

270. Indeed, the EDPB agrees with the FI SA that “If the IE SA does not make use of their respective corrective powers, there is danger that WhatsApp continues to unlawfully process personal data on the foot of Article 6(1)(b) GDPR” for service improvement and security

processing operations and “there is a danger that WhatsApp continues to undermine or bypass” data protection principles. In addition, failure to adopt any corrective measure in this case “would amount to a dangerous precedent, sending a deceiving message to the market and to data subjects, and would endanger the fundamental rights and freedoms of data subjects whose personal data are and will be processed by the controller”.

271. As a consequence, the EDPB finds it appropriate for an order to bring processing into compliance to be imposed in this case (without prejudice to the additional conclusions in respect of the imposition of administrative fines available below in Section 8).

272. According to the EDPB, the deadline for compliance with the order should be reasonable and proportionate, in light of the potential for harms to the data subject rights and the resources available to the controller to achieve compliance.

273. Finally, the EDPB recalls that non-compliance with an order issued by a supervisory authority can be relevant both in terms of it being subject to administrative fines up to 20.000.000 euros or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year in line with Article 83(6) GDPR, and in terms of it being an aggravating factor for the imposition of administrative fines.³³⁵ In addition, the investigative powers of supervisory authorities allow them to order the provision of all the information necessary for the performance of their tasks including the verification of compliance with one of their orders.

274. In light of the above, the EDPB instructs the IE SA to include in its final decision an order for WhatsApp IE to bring its processing of personal data for the purposes of service improvement and security features in the context of its Terms of Service into compliance with Article 6(1) GDPR in accordance with the conclusion reached by the EDPB³³⁷ within a specified period of time.”

8.2 As regards the deadline for compliance with the order that the Commission is required to impose, paragraph 272 of the Article 65 Decision provides that:

“... the deadline for compliance with the order should be reasonable and proportionate, in light of the potential for harms to the data subject rights and the resources available to the controller to achieve compliance”

8.3 Footnote 334 to the Article 65 Decision clarifies, in this regard, that:

"The EDPB recalls its Binding Decision 1/2021 adopted on 28 July 2021 where the EDPB was called to resolve a dispute pursuant to Article 65 GDPR concerning, among others, the appropriateness of the deadline for compliance suggested in the draft decision at stake. After highlighting the relevance of Recitals 129 as well as 148 GDPR for the imposition of corrective measures, the EDPB took into account the number of data subjects affected and the importance of the interest of affected data subjects in seeing the relevant provisions of the GDPR complied with in a short timeframe. While the EDPB also took note of the challenges highlighted by the controller, it found in that case that a compliance order with a three months' timeframe could not be considered disproportionate considering the infringement as well as the type of organization, its size and the means (including inter alia financial resources but also legal expertise) available to it. Consequently, the EDPB instructed the LSA to amend the draft decision by reducing the deadline for compliance from six months to three months. EDPB Binding Decision 1/2021, paragraphs 254-263."

8.4 The Commission notes that EDPB Binding Decision 1/2021 also concerned WhatsApp and, in these circumstances, the EDPB's observations, as regards the *"type of organisation, its size and the means (including inter alia financial resources but also legal expertise) available to it"* apply equally to the subject matter of this Section 8.

8.5 As regards the other factors referenced at footnote 334, the Commission notes the views of the EDPB, as set out in paragraph 269 of the Article 65 Decision, that:

"The EDPB agrees with the FISA that "the infringement cannot be consider as minor". The EDPB reiterates that lawfulness of processing is one of the fundamental pillars of the data protection law and considers that processing of personal data without an appropriate legal basis is a clear and serious violation of the data subjects' fundamental right to data protection. All violations of the GDPR should be accompanied by the imposition of appropriate corrective measures. This is all the more the case with the violation of a fundamental and core obligation such as lawfulness, especially when affecting a high number of data subjects and a large amount of personal data."

8.6 The Commission notes that the views expressed by the EDPB, above, concerning the characteristics of the Article 6(1) GDPR infringement, are very similar to those expressed on the same subject matter in its Binding Decision 1/2021 (and as repeated at footnote 334 to the Article 65 Decision). In the circumstances, the Commission proposed to include a 3-month deadline for compliance with the terms of the order, to commence from the day following the date of service of the Commission's final decision.

8.7 Accordingly, the Commission proposed to amend the Draft Decision to include an order to bring processing into compliance in the following terms:

- a) WhatsApp is hereby required to take the necessary action to bring its processing of personal data for the purposes of service improvement and security features (excluding

processing for the purpose of “IT Security” as defined by paragraph 90 of the Article 65 Decision) (“the **Processing**”) in the context of its Terms of Service into compliance with Article 6(1) GDPR in accordance with the conclusion reached by the EDPB, as recorded at paragraph 274 of the Article 65 Decision within a period of three months, commencing on the day following the date of service of the Commission’s final decision.

- b) More specifically, WhatsApp is required to take the necessary action to address the EDPB’s finding that WhatsApp is not entitled to carry out the Processing on the basis of Article 6(1)(b) GDPR, taking into account the analysis and views expressed by the EDPB in Section 4.4.2 of the Article 65 Decision. Such action may include, but is not limited to, the identification of an appropriate alternative legal basis, in Article 6(1) GDPR, for the Processing together with the implementation of any necessary measures, as might be required to satisfy the conditionality associated with that/those alternative legal basis/bases.

8.8 Following the amendment of the Draft Decision to take account of the EDPB’s Article 65 Decision, WhatsApp was invited to exercise its right to be heard in relation to those aspects of the Draft Decision in relation to which the Commission was required to make a final determination or, otherwise, to exercise its discretion. WhatsApp furnished its submissions on these matters under cover of letter dated 23 December 2022 (“the **Final Submissions**”). In response to the formulation of the proposed order to bring processing into compliance, WhatsApp furnished extensive submissions that were directed to the length of the proposed deadline for compliance, as follows:

- a) WhatsApp has, firstly, submitted that this inquiry relates to “*very different*” issues to those considered in the EDPB’s Binding Decision 1/2021 and “*the magnitude of work required to achieve compliance in this Inquiry is not comparable to that required in the WhatsApp Transparency Inquiry.*”⁶¹
- b) WhatsApp has, secondly, submitted⁶² that “*... work of this magnitude would generally require a period of at least nine to eleven months to implement, albeit with some potential to expedite aspects so that the work could conceivably be condensed into a six to nine month period.*”⁶³⁶⁴ WhatsApp has provided a relatively detailed assessment of the work required to be carried out, in this regard, and noted that the majority of the phases of work identified, “*by their nature, have to be conducted consecutively and not concurrently.*”

⁶¹ Final Submissions, paragraph 4.3.

⁶² Final Submissions, paragraphs 5.3 and 5.4

⁶³ Final Submissions, paragraph 4.5 and 5.5

⁶⁴ Final Submissions, paragraph 5.7

c) WhatsApp has, thirdly, submitted¹⁵⁸ that if it were forced to



d) WhatsApp, fourthly, submitted⁶⁵ that the proposed compliance period is inconsistent with the approaches taken by other supervisory authorities “in similar scenarios”, citing the examples of a decision in which the Luxembourgish supervisory authority afforded Amazon six months to rectify processing operations in relation to Articles 6, 12, 14, 15, 16, 17 and 21 GDPR and a decision in which the Belgian supervisory authority afforded IAB Europe a period of approximately eight months to bring its processing into compliance with Articles 5(1)(a) and 6 GDPR.

e) WhatsApp, fifthly, submitted⁶⁶ that the Article 65 Decision does not require the proposed order to take effect on “the day following the date of service of the [Commission’s] final decision, as originally proposed. It further submitted that, were a compliance order to be made in the terms proposed, this would require WhatsApp to dedicate its resources to attempting to comply with that order immediately given the excessively short compliance period. This would seriously impair and prejudice [WhatsApp’s] right to an effective appeal. To address this, WhatsApp submitted that the compliance period ought to run from the expiry of the statutory appeal period.

8.9 Having carefully considered the above submissions, I firstly note the size and considerable resources (both in terms of financial resourcing as well as personnel) that are available to WhatsApp. I further note that, further to the WhatsApp Transparency Decision, the originally proposed period for compliance with the relevant order was reduced from six to three months further to the EDPB’s Binding Decision 1/2021,⁶⁷ notwithstanding WhatsApp’s objection to same. I note that, despite those objections, WhatsApp achieved compliance with the order within the reduced compliance period.

⁶⁵ Final Submissions, paragraph 6.3

⁶⁶ Final Submissions, paragraphs 7.1, 7.3 and 7.4

⁶⁷ Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted 28 July 2021.

8.10 These factors notwithstanding, I cannot ignore the submissions that are summarised at paragraphs 8.8(a), (c) and (d), above. I agree that the infringements sought to be addressed by the within order are very different to those required to be addressed by the WhatsApp

Transparency Decision. I also consider it likely that the remedial work required to be carried out will be more extensive and significantly more complex than the work that was required to be carried out in the WhatsApp Transparency Decision. I have also taken account of the position, as regards the matters set out at paragraph 8.8(d), above. I further note the risks potentially associated with a position whereby WhatsApp is forced to make changes without adequate time to consider the consequences of those changes, as outlined at paragraph 8.8(c), above. Given that the objective sought to be achieved by the order is the protection of the fundamental rights and freedoms of data subjects, it would undermine that protection if, as a result of an inadequate period for compliance, data subjects were put at risk of other harms, such as those that might be presented by bad actors.

8.11 In the circumstances, I am persuaded that it is necessary for me to increase the previously proposed deadline for compliance, from a period of three to six months, commencing on the day following the date of service of this Decision on WhatsApp. This extension takes account of the significant financial, technological and human resources at WhatsApp's disposal. It further reflects the shortest period of time for compliance identified by WhatsApp in its submissions and, in these circumstances, it reflects a good balance, as between the need to protect the fundamental rights and freedoms of data subjects by bringing about the required changes to WhatsApp's processing of personal data and WhatsApp's entitlement to be made subject to measures that are no more than necessary to achieve the stated objective.

8.12 For the avoidance of doubt, I am not persuaded by the submissions summarised at paragraph 8.8(e), above. I note, in this regard, that WhatsApp has not explained how a shorter timeline for compliance would "seriously impair and prejudice" its right to an effective appeal. I further note that matters pertaining to the possible filing of any appeal will likely be dealt with by WhatsApp's internal and external legal advisors as opposed to the various technologists whose input will be required as part of WhatsApp's efforts to achieve compliance with the terms of the order. While I anticipate that there will, of course, be overlap in terms of the resources that might need to devote time to both the required remedial action and matters pertaining to the possible filing of any appeal, I do not envisage how such overlap would be anywhere near total such as to give rise to a risk to WhatsApp's ability to exercise its right to an effective appeal. I further note that the compliance deadline extends significantly beyond the limitation periods prescribed for any application for judicial redress under Irish law. In these circumstances, I am satisfied that WhatsApp's right to pursue judicial redress will not be impaired by the compliance period outlined above.

- 8.13 Accordingly, and having taken account of WhatsApp’s submissions, the Commission will include, as part of this Decision, an order requiring WhatsApp to bring its processing operations into compliance, in the terms outlined at paragraph 8.7 above, within a period of six months, commencing on the day following the date of service of this Decision on WhatsApp.

9 ADMINISTRATIVE FINE

9.1 The Article 65 Decision further includes a requirement for the Commission to impose an administrative fine in response to the EDPB's finding of infringement of Article 6(1) GDPR, as follows:

305. The EDPB concurs that the decision to impose an administrative fine needs to be taken on a case-by-case basis in light of the circumstances and is not an automatic one. However, the EDPB recalls that when a violation of the Regulation has been established, competent supervisory authorities are required to react appropriately to remedy this infringement in accordance with the means provided to them by Article 58(2) GDPR, which includes the possible imposition of an administrative fine pursuant to Article 58(2)(i) GDPR.

306. Indeed, as already mentioned the consistency mechanism may also be used to promote a consistent application of administrative fines: where a relevant and reasoned objection identifies shortcomings in the reasoning leading to the imposition of the fine at stake (or naturally the lack of one), the EDPB can instruct the LSA to engage in a new assessment of the need for a fine or the calculation of a proposed fine.

307. The EDPB again wants to recall that although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the processing of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence. Recital 148 shows the duty for supervisory authorities to impose corrective measures that are proportionate to the seriousness of the infringement.

308. With respect to the imposition of an administrative fine, the EDPB recalls the requirements of Article 83(1) GDPR, as well as that due account must be given to the elements of Article 83(2) GDPR.

309. As already established the EDPB considers the **lawfulness of processing** to be one of the fundamental pillars of the data protection law and that processing of personal data without an appropriate legal basis is a clear and serious violation of the data subjects' fundamental right to data protection. The EDPB therefore agrees with the FR SA in considering the identified breach as serious.

Furthermore, the EDPB takes the view that the infringement at issue relates to the processing of personal data of a significant number of people in a cross-border scope and that the impact on them has to be considered.

310. The EDPB underlines that the specific circumstances of the case have to be reflected. 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 size and financial position.

311. Though the **damage** is very difficult to express in terms of a monetary value, it remains the case that data subjects have been faced with data processing that should not have

occurred (by relying inappropriately on Article 6(1)(b) GDPR as a legal basis as established in section 4.4.2). The data processing in question entails decisions about information that data subjects are exposed to or excluded from receiving. The EDPB recalls that non-material damage is explicitly regarded as relevant in recital 75 GDPR and that such damage may result from situations “*where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data*”. Given the nature and gravity of the infringement of Article 6(1) GDPR, a risk of damage caused to data subjects is, in such circumstances, consubstantial with the finding of the infringement itself.

312. In the light of the **nature and gravity of the infringement** pursuant to Article 83(2)(a) GDPR as identified in the paragraphs above, in the view of the EDPB the combination of the mentioned factors already clearly tip the balance in **favour of imposing an administrative fine**.

313. For conduct infringing data protection rules, the GDPR does not provide for a minimum fine. Rather, the GDPR only provides for maximum amounts in Article 83(4)–(6) GDPR, in which several different types of conduct are grouped together. A fine can ultimately only be calculated by weighing up all the elements expressly identified in Article 83(2)(a)–(j) GDPR, relevant to the case and any other relevant elements, even if not explicitly listed in the said provisions (as Article 83(2)(k) GDPR requires to give due regard to any other applicable factor). Finally, the final amount of the fine resulting from this assessment must be effective, proportionate and dissuasive in each individual case (Article 83(1) GDPR). Any fine imposed must sufficiently take into account all of these parameters, whilst at the same time not exceeding the legal maximum provided for in Article 83(4)–(6) GDPR.

314. In light of the above, the **EDPB instructs the IE SA to impose an administrative fine**, remaining in line with the criteria provided for by Article 83(2) GDPR and ensuring it is effective, proportionate and dissuasive in line with Article 83(1) GDPR, in accordance with the conclusions reached by the EDPB, namely the identified infringement of Article 6(1) GDPR.

9.2 The Article 65 Decision further provides, in relation to the infringement that was found to have occurred of the Article 5(1)(a) fairness principle, that:

315. The EDPB recalls its conclusion in this Binding Decision on the infringement by WhatsApp IE of the fairness principle under Article 5(1)(a) GDPR and that the objection raised by the IT SA, which is found to be relevant and reasoned, requested the IE SA to exercise its power to impose an administrative fine.

316. The EDPB takes note of WhatsApp IE’s view that the IT SA objection is not relevant and reasoned and also notes that WhatsApp IE takes that view that inappropriate, clearly disproportionate, and unnecessary to impose an administrative fine.

317. The EDPB again recalls that the decision to impose an administrative fine needs to be taken on a case-by-case basis in light of the circumstances and is not an automatic one and the specificities of the case have to be taken into account.

318. As previously established, the principle of fairness under Article 5(1)(a) GDPR, although intrinsically linked to the principles of lawfulness and transparency under the same provision, has an independent meaning.

319. Considering the EDPB's findings in Section 5.4.2 that WhatsApp IE has not complied with key requirements of the principle of fairness, the EDPB reiterates its view that WhatsApp IE has infringed the principle of fairness under Article 5(1)(a) GDPR and agrees with the IT SA that this infringement should be adequately taken into account by the IE SA in the calculation of the amount of the administrative fine to be imposed following the conclusion of this inquiry.

320. Therefore, the EDPB instructs the IE SA to take into account the infringement by WhatsApp IE of the fairness principle enshrined in Article 5(1)(a) GDPR as established above when determining the fine for the violation of Article 6(1) GDPR as instructed above. If, however, the IE SA considers an additional fine for the breach of the principle of fairness is an appropriate corrective measure, the EDPB requests the IE SA to include this in its final decision. In any case, the IE SA must take into account the criteria provided for by Article 83(2) GDPR and ensuring it is effective, proportionate and dissuasive in line with Article 83(1) GDPR.

- 9.3 For the avoidance of doubt, the Commission does not consider an additional fine for the breach of the principle of fairness that was established by the Article 65 Decision to be an appropriate corrective measure. The Commission notes, in this regard, that the EDPB's finding of infringement of the Article 5(1)(a) fairness principle was largely based on the lack of transparency, as regards the information that was presented to the data subject concerning the processing that would be carried out further to the Terms of Service (see, for example, paragraph 154 of the Article 65 Decision). The Commission previously imposed administrative fines totalling €225 million on WhatsApp by way of the WhatsApp Transparency Decision, arising from findings of infringement of Articles 5(1)(a), 12, 13 and 14 GDPR. Those findings of infringement concerned the same privacy policy referenced by the EDPB in its Article 65 Decision. In the circumstances, the imposition of a fine for the finding of infringement of the Article 5(1)(a) fairness principle would risk punishing WhatsApp twice for the same wrongdoing.

"THE PROCESSING CONCERNED"

- 9.4 For the purpose of the following assessment of the Article 83(2) criteria, "the processing concerned" should be understood as meaning the processing carried out by WhatsApp for the purpose of service improvement and security features (excluding "IT Security", as described in paragraph 90 of the Article 65 Decision) in the context of its Terms of Service. This reflects the scope of the finding of infringement of Article 6(1) GDPR, as set out in paragraph 122 of the Article 65 Decision.

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:

Nature

9.5 Paragraph 309 of the Article 65 Decision records the EDPB's view that:

"As already established the EDPB considers the lawfulness of processing to be one of the fundamental pillars of the data protection law and that processing of personal data without an appropriate legal basis is a clear and serious violation of the data subjects' fundamental right to data protection. The EDPB therefore agrees with the FR SA in considering the identified breach as serious."

9.6 It is therefore clear that the EDPB considers the Article 6(1) infringement to concern one of the "fundamental pillars" of the GDPR. The Commission further notes, in this regard, that paragraphs 312 and 328(14) of the Article 65 Decision indicate that the EDPB considered the nature of the infringement to be significant, in the context of its conclusion that an administrative fine ought to be imposed in relation to the infringement of Article 6(1) GDPR.

Gravity

9.7 The Article 65 Decision does not identify, with any particularisation, the EDPB's position on the gravity of the Article 6(1) infringement. The Commission notes, however, that paragraphs 312 and 328(14) of the Article 65 Decision indicate that the EDPB considered the gravity of the infringement to be significant, in the context of its conclusion that an administrative fine ought to be imposed in relation to the infringement of Article 6(1) GDPR.

9.8 The Commission, for its part, notes that infringements of Article 6 are subject to the higher fining threshold set out in Article 83(5) GDPR. The maximum fine prescribed by Article 83(5) GDPR is twice that prescribed by Article 83(4) GDPR. This arrangement clearly indicates that the legislator considered the matters covered by Article 83(5) GDPR to be particularly significant in the context of the data protection framework as a whole.

Duration

9.9 The Article 65 Decision does not contain any indication in relation to the manner in which the EDPB took account of the duration of the Article 6(1) infringement. The Commission notes that the infringement has occurred since 25 May 2018 and remains ongoing.

Number of data subjects affected

9.10 Paragraph 309 of the Article 65 Decision records the EDPB's view that:

"the infringement at issue relates to the processing of personal data of a significant number of people in a cross-border scope ..."

Level of damage suffered by them

9.11 Paragraph 311 of the Article 65 Decision records that:

"Though the damage is very difficult to express in terms of a monetary value, it remains the case that data subjects have been faced with data processing that should not have occurred The data processing in question entails decisions about information that data subjects are exposed to or excluded from receiving. The EDPB recalls that non-material damage is explicitly regarded as relevant in Recital 75 and that such damage may result from situations "where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data". Given the nature and gravity of the infringement of Article 6(1) GDPR, a risk of damage caused to data subjects is, in such circumstances, consubstantial with the finding of the infringement itself."

9.12 Paragraph 120 of the Article 65 Decision considers the risks arising from the Article 6(1) infringement as follows:

"Some of the safeguards from which data subjects would be deprived due to an inappropriate use of Article 6(1)(b) GDPR as legal basis, instead of others such as consent under Article 6(1)(a) GDPR and legitimate interest under Article 6(1)(f) GDPR, are the possibility to specifically consent to certain processing operations and not to others and to the further processing of their personal data (Article 6(4) GDPR; their freedom to withdraw consent (Article 7 GDPR); their right to be forgotten (Article 17 GDPR); and the balancing exercise of the legitimate interests of the controller against their interests or fundamental rights and freedoms (Article 6(1)(f) GDPR)."

9.13 It therefore appears that the EDPB considered the infringement to give rise to a risk of loss of control over, and ability to exercise choice concerning, one's personal data. This is consistent with the complainant's position that the infringement had the effect of negating her free will (see point ii, page 16 of the complaint).

9.14 The Commission notes, in this regard, that Recital 75 (which acts as an aid to the interpretation of Article 24 GDPR, 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]

- 9.15 The Commission further considers that the infringement of the Article 5(1)(a) fairness principle may be taken into account, as required by the Article 65 Decision, under this particular heading. The Commission notes, in this regard, paragraph 153 of the Article 65 Decision, which records the EDPB’s position that:

“ ... the EDPB shares the IT SA’s concern that WhatsApp IE misrepresented the legal basis of the processing and that WhatsApp IE’s users are left “in the dark” as to the possible connections between the purposes sought, the applicable legal basis and the relevant processing activities. This being said, the EDPB considers that the processing by WhatsApp IE cannot be regarded as ethical and truthful because it is confusing with regard to the type of data processed, the legal basis used and the purposes of the processing, which ultimately restricts the WhatsApp IE’s users’ possibility to exercise their data subjects’ rights.”

- 9.16 On the basis of the views that have been expressed by the EDPB, as recorded above, the Commission concludes that the infringement of Article 6(1) GDPR falls within the upper range of the scale, in terms of seriousness, for the purpose of the assessment of the Article 83(2)(a) criterion

WhatsApp’s Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

- 9.17 As noted previously, following the amendment of the Draft Decision to take account of the EDPB’s Article 65 Decision, WhatsApp was invited to exercise its right to be heard in relation to those aspects of the Draft Decision in relation to which the Commission was required to make a final determination or, otherwise, to exercise its discretion. WhatsApp furnished its submissions on these matters under cover of letter dated 23 December 2022 (“the Final Submissions”).
- 9.18 In relation to the nature of the Article 6(1) infringement, WhatsApp “respectfully [urged] the [Commission] not to rely on the EDPB’s erroneous decision with respect to Article 83(2)(a) GDPR, in light of [identified] significant errors in the EDPB’s reasoning.¹⁶²” WhatsApp further submitted, in this regard, that the EDPB’s conclusion was “not correct and not supported by the evidence”¹⁶³.
- 9.19 WhatsApp further submitted¹⁶⁴ that it has “at all times relied openly and in good faith on Article 6(1)(b) GDPR in respect of the Processing and was supported, in principle, in this reliance by the

¹⁶² Final Submissions, paragraph 10.4

¹⁶³ Final Submissions, paragraph 10.6

¹⁶⁴ Final Submissions, paragraph 10.6

initial findings of the [Commission]. [WhatsApp's] good faith reliance on Article 6(1)(b) GDPR in these circumstances must be regarded as a very significant mitigating factor. It was only during the Article 60 GDPR process that a difference of view emerged between the [Commission] and CSAs regarding Article 6(1)(b) GDPR which required resolution by the EDPB." Furthermore, it submitted⁶⁸ that the "Article 65 Decision also relies on the Contractual Necessity Guidelines. However, these guidelines do not address security related processing. Furthermore, the Guidelines should not be relied on at all in circumstances where they were not adopted until after this Inquiry commenced. To the extent that guidance postdating the commencement of the Inquiry is being used to retrospectively characterise the nature of the purported infringement, this is fundamentally unfair and in breach of legal certainty."

9.20 In circumstances where the Article 65 Decision is binding upon the Commission, I am not in a position to act contrary to, or otherwise look behind, the views that have been so expressed the EDPB. The EDPB has clearly set out its views, in this regard, at paragraph 309 of the Article 65 Decision, as quoted above. In the circumstances, I cannot consider the infringement as being anything less than serious in nature.

9.21 In relation to the **gravity** of the Article 6(1) infringement, WhatsApp submitted⁶⁹ that it would be inappropriate for the Commission, in reaching its own determination to afford any weight to the EDPB's decision on gravity of the infringement. Furthermore, the inclusion of reference to Article 6 GDPR in the list of infringements that are covered by the higher of the two fining "cap" provisions "cannot justify a finding of significant gravity in this instance" in circumstances where Article 83 requires this assessment to take account of the relevant factors in "each individual case⁷⁰". WhatsApp submitted⁷¹, in this regard, that the gravity of the infringement should properly be characterised as minor, taking into account the fact that: (i) the processing is not intrusive in nature; (ii) limited categories of data are processed by WhatsApp to provide the WhatsApp Service; and (iii) the processing at issue was conducted for the purpose of keeping data subjects safe and providing them with a product that met their expectations.

9.22 WhatsApp further considered it "significant" that neither the Commission nor the Article 65 Decision prohibit it from engaging in the processing – either on a temporary or permanent basis. *"Rather, they require WhatsApp to identify an appropriate legal basis for the processing. It is respectfully submitted that, with this factual context in mind, the*

⁶⁸ Final Submissions, paragraph 10.6

⁶⁹ Final Submissions, paragraph 10.9

⁷⁰ Final Submissions, paragraph 10.11

⁷¹ Final Submissions, paragraph 10.12

gravity of the infringement in this instance cannot be on the upper end of the potential infringements that could fall within the broad categories laid out in Article 83(5).⁷²

- 9.23 As before, the Commission is not in a position to act contrary to the views that have been clearly expressed by the EDPB in its binding Article 65 Decision. As already acknowledged, the EDPB has not elaborated on the reasons why it considers the gravity of the Article 6(1) infringement to be one of the factors that tip the balance in favour of the imposition of a fine. This does not alter the fact, however, that the EDPB clearly considered the gravity of the Article 6(1) infringement to be of one of the factors that warranted the imposition of an administrative fine. In these circumstances, it is not open to the Commission to conclude that the gravity of the infringement is not significant, in terms of its impact on the overall assessment of the Article 83(2)(a) criterion.
- 9.24 Furthermore, it is appropriate for the Commission to have regard to the placement of an infringement, as between the infringements that are subject to Article 83(4) GDPR and those that are subject to Article 83(5) GDPR, in circumstances where this placement provides insight into the thinking of the EU legislator, as regards the gravity of infringements of particular provisions.
- 9.25 In relation to the significance of the absence of a ban on processing, the Commission notes that the purpose of an administrative fine is to sanction wrongdoing that has occurred. Measures such as a ban or an order to bring processing into compliance, however, serve a different purpose in that they are directed to addressing the wrongdoing on a forward-looking basis. Furthermore, when exercising corrective powers, supervisory authorities should not exceed what is necessary to achieve the stated objective. As noted above, the EDPB, in the Article 65 Decision, directed the Commission to address the Article 6(1) infringement by making an order to bring processing into compliance and to impose an administrative fine. Those directions reflect the EDPB's view that such measures do not exceed what is necessary to address the infringements that were found to have occurred. It would be incorrect, however, to equate the choice of measures as being indicative of the EDPB's position on the gravity of the infringements themselves. In the circumstances, and notwithstanding the absence of a ban, it cannot be suggested that the EDPB considered the infringement to be "minor", as suggested by WhatsApp.
- 9.26 In relation to the **duration** of the Article 6(1) infringement, WhatsApp has submitted that the duration of the infringement "*... should not be considered to support the conclusion that the infringement of Article 6(1) GDPR falls within the 'upper range of the scale'*", in terms of seriousness.⁷³ In the absence of any specific direction from the EDPB, in this

⁷² Final Submissions, paragraph 10.13

⁷³ Final Submissions, paragraph 10.16.

regard, the Commission has not allocated this factor with any significant weight, in terms of its impact on the overall assessment of the Article 83(2)(a) criterion.

9.27 In relation to the **number of data subjects affected and the level of damage suffered by them**, WhatsApp has submitted that:

- *“the [Commission] should not rely on paragraph 309 of the Article 65 Decision where it states that “the infringement at issue relates to the processing of personal data of a significant number of people in a cross-border scope ...” given that no investigation has been carried out by either the [Commission] or the EDPB as to the relevant Processing or in turn how many data subjects are impacted⁷⁴”*
- *“the only data subject who is relevant for the purpose of Article 83(2)(a) is the data subject represented by the Complainant and any consideration of the level of damage suffered is confined to a consideration of any damage the Complainant may have suffered. At no point in the Inquiry has the Complainant offered any evidence to demonstrate that the data subject represented by it has suffered damage, and no evidence of any such damage has otherwise been adduced in the Inquiry.¹⁷²”*
- *“... even if it is open to the [Commission] to consider whether other data subjects have been affected and to have regard to any damage suffered by them, there is no evidence whatsoever in this Inquiry that any other data subjects have suffered any damage. To the contrary, the Processing was conducted for the purposes of keeping the service users signed up for safe and evolving to meet their expectations⁷⁵.”*

9.28 In response to the above submissions, it is, firstly, important to note that the Commission is subject to a binding decision of the EDPB, which includes an assessment of the damage suffered by data subjects, at paragraph 311 thereof. In the circumstances, it is not open to the Commission to find that no damage has been suffered. Secondly, the Complainant herself identified the damage that she alleges to have suffered in connection with the matters which formed the basis for the EDPB’s findings of infringement of Article 6(1) and the Article 5(1)(a) principle of fairness. Thirdly, as regards the damage suffered by data subjects other than the Complainant, the matters covered by the findings of infringement are not matters on which any individual user of WhatsApp has the power to exercise choice (other than, of course, the choice to use WhatsApp or not). Where any individual data subject chooses to use WhatsApp, the basic processing that takes place (the subject of the within Inquiry) is the same as that applied to the personal data of the Complainant. In these circumstances, it cannot be said that the identified damage suffered, i.e. loss of

⁷⁴ Final Submissions, paragraph 10.18 ¹⁷²

Final Submissions, paragraph 10.19

⁷⁵ Final Submissions, paragraph 10.20

control over one's personal data, is limited to the Complainant alone. For these reasons, it is appropriate for the Commission to take account of the damage suffered by all user data subjects as part of the Article 83(2) assessment.

- 9.29 Having taken account of the Final Submissions, I remain of the view that the infringement of Article 6(1) GDPR falls within the upper range of the scale, in terms of seriousness, for the purpose of the assessment of the Article 83(2)(a) criterion.

ARTICLE 83(2)(B): INTENTIONAL OR NEGLIGENT CHARACTER OF INFRINGEMENT

9.30 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes that, at paragraph 56 its Fining Guidelines 04/2022, the EDPB restates the position that *"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."*

9.31 The Fining Guidelines, at paragraph 57, further provide that *"(t)he intentional or negligent character of the infringement ... should be assessed taking into account the objective elements of conduct gathered from the facts of the case."*

9.32 There is nothing, in the EDPB's assessment of the objective elements of conduct gathered from the facts of the case, to suggest that the Article 6(1) GDPR infringement was intentional on the part of WhatsApp. In the circumstances, the Commission considers the infringement to be negligent in character. The Commission notes the views expressed by the EDPB in its Fining Guidelines 04/2022, that *"(a)t best, negligence could be regarded as neutral"* and, accordingly, the Commission proposes to treat this factor as neither mitigating nor aggravating.

WhatsApp's Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

9.33 By way of the Final Submissions, WhatsApp relies in part on its submissions on the nature of the infringement, which I have considered in the context of my analysis of Article 83(2)(a) GDPR above. WhatsApp also submitted that:

"... it became clear in the course of the Article 60 process that there was a reasonably held difference of views between the [Commission] and certain of the CSAs regarding Article 6(1)(b) GDPR which required resolution by the EDPB. Where there is such a clear disagreement as to the correct interpretation and/or application of Article 6(1) GDPR – for

example, where supervisory authorities themselves disagree as to the approach adopted – any subsequent finding of infringement should not be characterised as negligent.”⁷⁶

9.34 In reliance on the above, WhatsApp submitted⁷⁷ that this alleged lack of negligence ought to be recognised in this Decision and the fine reduced accordingly.

9.35 While I acknowledge WhatsApp’s position, in this regard, I am bound to adopt this Decision in a manner that is consistent with the views that have been expressed by the EDPB in the Article 65 Decision. I note, in this regard, that the EDPB placed reliance⁷⁸ on guidance that it issued in 2019⁷⁹, as part of the assessment that resulted in a finding of infringement of Article 6(1) GDPR.

9.36 In the circumstances, and acknowledging WhatsApp’s genuinely held view, I do not believe that it would be consistent with the Article 65 Decision for me to conclude that the infringement ought properly to be classified as neither negligent nor intentional in character simply because of a genuinely held belief, on the part of WhatsApp, in its entitlement to rely on Article 6(1)(b) GDPR to carry out the processing concerned. The references to the 2019 guidelines in the Article 65 Decision indicate that the EDPB considers its position on the matter to have been clear since that time. I am further of the view that, had the EDPB considered the infringement to be neither negligent nor intentional in character, this would have been reflected in the determination, by the EDPB, that resulted in the direction that required the imposition of an administrative fine. My view, in this regard, is that an infringement which has been characterised as neither intentional nor negligent would likely weigh heavily against the question of whether, by reference to Article 83(2), the imposition of an administrative fine might be warranted in the circumstances of a particular case.

9.37 For the reasons outlined above, I am not satisfied that it would be appropriate for me, in the circumstances of this Decision, to depart from the position reflected in the EDPB’s Fining Guidelines 04/2022, that “(a)t best, negligence could be regarded as neutral”. Accordingly, and having considered WhatsApp’s position on the matter, I remain of the view that the infringement ought properly to be characterised as negligent and that this factor is neither mitigating nor aggravating in the circumstances of the case.

ARTICLE 83(2)(c): ANY ACTION TAKEN BY THE CONTROLLER TO MITIGATE THE DAMAGE SUFFERED BY DATA SUBJECTS

⁷⁶ Final Submissions, paragraph 10.26.

⁷⁷ Final Submissions, paragraph 10.27

⁷⁸ See, for example, paragraphs 104 and 112 of the Article 65 Decision

⁷⁹ 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 2.0, 8 October 2019

9.38 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes that WhatsApp, throughout the course of the inquiry, considered that it was entitled to process personal data for service improvement and security purposes in reliance on Article 6(1)(b) GDPR. That being the case, it follows that WhatsApp could not have been expected to take action “to mitigate the damage suffered by data subjects” in circumstances where WhatsApp did not consider any infringement to have occurred or any damage to have been suffered by data subjects. In the circumstances, the Commission considers this factor to be neither aggravating nor mitigating.

WhatsApp’s Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

9.39 By way of the Final Submissions, WhatsApp has urged me to take account of various mitigating matters, namely that:

“(i) at all relevant times WhatsApp Ireland believed, and had a reasonable basis to believe, that reliance on Article 6(1)(b) was appropriate in principle; (ii) there is no evidence of any damage to data subjects; and (iii) WhatsApp Ireland made a number of changes to improve transparency for users to the satisfaction of the [Commission] and CSAs (which the EDPB alleges underpins the Article 6(1) infringement)”.⁸⁰

9.40 On the basis of the above, WhatsApp has submitted⁸¹ that this should be treated as a mitigating factor.

9.41 I note that I have already addressed WhatsApp’s submissions concerning the absence of evidence of damage, as part of the Article 83(2)(a) GDPR assessment. In relation to the identified changes made to improve transparency for users, I note that WhatsApp was subject to an obligation to make those changes (by virtue of the order made pursuant to the WhatsApp Transparency Decision). As regards the significance of those changes in the context of the infringement of Article 6(1) under assessment, it is clear (from the Article 65 Decision) that the rectification of the transparency deficits that were identified by the WhatsApp Transparency Decision do not address the damage suffered by data subjects arising from the Article 6(1) infringement (as considered within the Article 83(2)(a) criterion, above). In the circumstances, I am unable to take account of such matters as mitigating factors in relation to the mitigation of damage suffered by data subjects as a result of the infringement of Article 6(1) GDPR.

⁸⁰ Final Submissions, paragraph 10.29.

⁸¹ Final Submissions, paragraph 10.29

9.42 Accordingly, and having considered WhatsApp’s position in this regard, I remain of the view that this factor ought to be treated as neither mitigating nor aggravating for the reasons set out at paragraph 9.38, above.

ARTICLE 83(2)(D): THE DEGREE OF RESPONSIBILITY OF THE CONTROLLER, TAKING INTO ACCOUNT TECHNICAL AND ORGANISATIONAL MEASURES IMPLEMENTED BY THEM PURSUANT TO ARTICLES 25 AND 32

9.43 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. Given that the extent to which WhatsApp might comply with its obligations pursuant to Articles 25 and 32 was not required to be examined by the inquiry, the Commission considers this factor to be neither mitigating nor aggravating. WhatsApp, by way of the Final Submissions, confirmed⁸² its agreement with the above approach. In the circumstances, I conclude that this factor is neither mitigating nor aggravating.

ARTICLE 83(2)(E): ANY RELEVANT PREVIOUS INFRINGEMENTS BY THE CONTROLLER

9.44 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes the findings of infringement previously recorded against WhatsApp in the Transparency Decision. That decision concerned an in-depth assessment of the extent to which WhatsApp complied with its transparency obligations and recorded findings of infringement of Articles 5(1)(a), 12, 13 and 14 GDPR. The Commission notes, however, the overlap in temporal scope and subject matter, as between that decision and the within one. The Commission notes, in particular, the fact that the Transparency Decision was the result of an own-volition inquiry that was commenced at the same time as the inquiry underlying this decision. The fact that there are previous infringements in existence is a consequence of the fact that the inquiry underlying the Transparency Decision reached completion ahead of the within inquiry. The Commission’s view is that the word “previous” in the text of Article 83(2)(e) indicates a requirement for temporal separation between the conduct giving rise to a previously established finding of infringement and the conduct under present assessment. The infringements established by the Transparency Decision do not reflect earlier offending on the part of WhatsApp. In these particular circumstances, and without prejudice to the question of whether or not the infringements recorded in the Transparency Decision are “relevant” for the purpose of Article 83(2)(e) GDPR, the Commission considers this factor to be neither mitigating nor aggravating.

WhatsApp’s Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

⁸² Final Submissions, paragraph 10.30.

9.45 WhatsApp, by way of the Final Submissions, disagrees with the above and, instead, urges the Commission to treat this factor as mitigating, in line with the Commission's approach in other (named) inquiries.⁸³ I note, in this regard, that the named inquiries do not concern cross-border processing.

9.46 In response to the above, 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) GDPR 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, inhouse, compliance teams. Such entities 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 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, nor the Commission's decision in the WhatsApp Transparency Decision, nor the Facebook (12 breaches) inquiry. The Commission's approach to the Article 83(2) GDPR assessment, as recorded in these decisions (amongst others), is consistent with that applied to the within inquiry. Accordingly, I remain of the view that this factor ought to be treated as neither mitigating nor aggravating.

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

9.47 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. In the circumstances, the Commission proposes to consider this factor to be neither mitigating nor aggravating for the same reasons set out in the Article 83(2)(c) assessment, above.

WhatsApp's Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

9.48 By way of the Final Submissions, WhatsApp has submitted that I should treat this factor as mitigating in light of the fact that it has taken "... various steps (along with its historic approach of voluntary engagement and cooperation with the [Commission]) to improve transparency for its users...and

⁸³ Final Submissions, paragraphs 10.31-10.33.

will undertake all efforts to comply with any order issued by the [Commission], as required.”⁸⁴
WhatsApp further submits that it has also cooperated fully with the Commission throughout the Inquiry.

9.49 While the Commission recognises that WhatsApp has cooperated fully throughout the Inquiry, the Commission notes that WhatsApp is obliged to do so by virtue of Article 31 GDPR. Furthermore, and while the Commission acknowledges WhatsApp’s commitment to undertake “*all efforts to comply with any order*” that might be issued further to this Decision, I again note that WhatsApp is subject to an obligation to comply with the terms of the relevant order. In relation to the steps taken to improve transparency for users, I note that I have already addressed such submissions further to the Article 83(2)(c), above.

9.50 Accordingly, I remain of the view that this factor ought to be treated as neither mitigating nor aggravating.

ARTICLE 83(2)(G): THE CATEGORIES OF PERSONAL DATA AFFECTED BY THE INFRINGEMENT

9.51 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes, further to the corresponding assessment in the Transparency Decision, that the categories of personal data that WhatsApp processes for the purpose of delivering its service are not extensive. The Commission is cognisant, however, of the fact that the inquiry underlying this decision did not include an examination of the specific categories of personal data being processed by WhatsApp for service improvement and security purposes. In the circumstances, the Commission proposes to consider this factor as a mitigating factor of the lightest possible weight.

WhatsApp’s Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

9.52 By way of the Final Submissions, WhatsApp submits that greater mitigating weight should be afforded to this factor.⁸⁵ It submits that the Commission “... *has not specifically investigated the categories of personal data affected by the Processing, and so the basis for its conclusion is unclear.*”⁸⁶ WhatsApp further submits that the processing in question is not intrusive, and that it is not capable of giving rise to damage, both in light of the limited categories of data being processed, and “... *various privacy-protective measures it has in place, such as end-to-end encryption.*”⁸⁷

⁸⁴ Final Submissions, paragraph 10.35.

⁸⁵ Final submissions, paragraph 10.37.

⁸⁶ Final Submissions, paragraph 10.38.

⁸⁷ Final Submissions, paragraph 10.39.

9.53 As already acknowledged, the scope of the complaint, as originally assessed by the Commission, did not necessitate investigation of the specific processing operations or categories of personal data undergoing processing. This notwithstanding, the Commission considers that it can discern sufficient information from the Privacy Policy to sustain the conclusion proposed above that the categories of personal data affected by the Article 6(1) GDPR infringement are not extensive. Such a conclusion is also consistent with the outcome of the same assessment, as reflected in the WhatsApp Transparency Decision (noting that the same Privacy Policy underpinned both the WhatsApp Transparency Decision and this Decision).

9.54 As regards WhatsApp's submission that I should afford greater mitigating weight to this factor, I note that WhatsApp has not provided me with any basis that would enable me to do so. While I acknowledge its submissions considering the various "privacy-protective measures" it has in place, the focus of Article 83(2)(g) is the "categories" of personal data affected by the infringement. In the absence of submissions directed to this specific point, I remain of the view that this factor ought to be treated as a mitigating factor of the lightest possible weight.

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 NOTIFIED THE INFRINGEMENT

9.55 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes that the subject-matter of the inquiry did not give rise to any obligation on the part of WhatsApp to make a formal notification to the Commission. Accordingly, the Commission proposes to consider this factor as neither mitigating nor aggravating. WhatsApp, by way of the Final Submissions, confirmed⁸⁸ its agreement with the above approach. In the circumstances, I conclude that this factor is neither mitigating nor aggravating.

ARTICLE 83(2)(I): WHERE MEASURES REFERRED TO IN ARTICLE 58(2) HAVE PREVIOUSLY BEEN ORDERED AGAINST THE CONTROLLER CONCERNED WITH REGARD TO THE SAME SUBJECT-MATTER, COMPLIANCE WITH THOSE MEASURES

9.56 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes that measures have not previously been ordered against WhatsApp with regard to the same subject matter. In the circumstances, the Commission proposes to consider this factor as neither mitigating nor aggravating. WhatsApp, by way of the Final Submissions, confirmed⁸⁹ its agreement with the above approach. In the circumstances, I conclude that this factor is neither mitigating nor aggravating.

⁸⁸ Final Submissions, paragraph 10.40.

⁸⁹ Final Submissions, paragraph 10.41.

ARTICLE 83(2)(J): ADHERENCE TO APPROVED CODES OF CONDUCT PURSUANT TO ARTICLE 40 OR APPROVED CERTIFICATION MECHANISMS PURSUANT TO ARTICLE 42

9.57 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission proposes to consider this factor as neither mitigating nor aggravating in circumstances where nothing arises for assessment under this heading. WhatsApp, by way of the Final Submissions, confirmed⁹⁰ its agreement with the above approach. In the circumstances, I conclude that this factor is neither mitigating nor aggravating.

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

9.58 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The Commission notes, however, the EDPB's view, as set out in the EDPB's binding decision 1/2021 (paragraphs 409 to 412, inclusive), that the turnover of the undertaking concerned ought to be taken into account not just for the calculation of the applicable fining "cap" but also for the purpose of assessing the quantum of the administrative fine itself. This position is further reflected in the Fining Guidelines 04/2022 (see, for example, paragraph 49). The Commission's assessment of the undertaking concerned and the applicable turnover figure is detailed below. While this is not a matter that can properly be classified as either mitigating or aggravating, by reference to the circumstances of the case, the Commission proposed to take the significant turnover of the undertaking concerned into account when determining the quantum of the proposed fine, as set out below.

WhatsApp's Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(2) GDPR, as introduced to this Decision following the adoption of the Article 65 Decision

9.59 By way of the Final Submissions, WhatsApp has submitted that *"the relevant "undertaking" for determining the fining cap is WhatsApp Ireland alone. Furthermore, the [Commission]'s consideration of turnover in the calculations of the fining range is incompatible with Article 83(2) GDPR and constitutes a clear error of law."*⁹¹ I note that WhatsApp has made further submissions on this aspect of matters, which are addressed further below, as part of the assessment of the applicable fining "cap".

9.60 As already noted above, the requirement to have regard to the turnover of the undertaking concerned in calculating the amount of the fine was previously determined by the EDPB in Binding Decision 1/2021. Furthermore, the meaning of "undertaking", as it appears in Article 83 and Recital 150 GDPR, is also the subject of previous EDPB determinations (including Binding Decision

⁹⁰ Final Submissions, paragraph 10.42.

⁹¹ Final Submissions, paragraph 10.44.

1/2021). In the circumstances, it is not open to the Commission to disregard these requirements. Accordingly, and while this is not a matter that can properly be classified as either mitigating or aggravating by reference to the circumstances of the case, the Commission has taken the significant turnover of the undertaking concerned into account when determining the quantum of the proposed fine, as set out below.

Summary

9.61 By reference to the above, the Commission concludes that:

- (i) The infringement of Article 6(1) GDPR (and taking into account the infringement of the Article 5(1)(a) fairness principle) has been assessed as falling at the upper end of the scale, in terms of seriousness, for the purpose of Article 83(2)(a).
- (ii) The categories of personal data affected by the Article 6(1) GDPR infringement ought to be taken into account as a mitigating factor of the lightest possible weight.
- (iii) Otherwise, the assessments of the Article 83(2)(b), 83(2)(c), 83(2)(d), 83(2)(e), 83(2)(f), 83(2)(h), 83(2)(i), 83(2)(j) and 83(2)(k) criteria are to be treated as neither mitigating nor aggravating for the purpose of the Article 6(1) GDPR infringement.

Outcome

9.62 On the basis of the above, I proposed to impose an administrative fine of an amount falling within the range of €5 million and €9 million, in respect of the infringement of Article 6(1) GDPR (and taking into account the infringement of the Article 5(1)(a) fairness principle).

9.63 The Commission expressed the view that an administrative fine of this nature would satisfy the requirement in Article 83(1) GDPR for any administrative fine imposed to be effective, proportionate and dissuasive in each individual case. In this regard, I have taken account of:

- (a) The purpose of the fine, which is to sanction the infringement of Article 6(1) (and taking into account the infringement of the Article 5(1)(a) fairness principle) that was found to have occurred (by the EDPB in the Article 65 Decision);
- (b) The requirement for any fine to be effective. In this regard, the Commission notes that the fine proposed above reflects the circumstances of the case, including both the specific elements of the infringement as well as those elements that relate to the controller which committed the infringement, namely its financial position (as required by paragraph 414 of the EDPB's binding decision 1/2021);

- (c) The requirement for a genuinely deterrent effect, in terms of discouraging both WhatsApp and others from committing the same infringement in the future;
- (d) The requirement for any fine to be proportionate and to not exceed what is necessary to achieve the stated objective (as recorded at a., above). The Commission considers that the fine proposed is proportionate to the circumstances of the case, taking into account the gravity of the infringements and all of the elements that may lead to an increase (aggravating factors) or decrease (mitigating factors) of the initial assessment as well as the significant turnover of the undertaking concerned. The fine also takes account of the fact that the fine will be imposed in addition to an order requiring WhatsApp to take action to bring its processing into compliance;
- (e) I have also taken particular account, in this regard, of the facts that:
 - i. The EDPB's finding of infringement of Article 6(1) GDPR was largely based on the lack of transparency, as regards the information that was presented to the data subject concerning the processing that would be carried out further to the Terms of Service.
 - ii. The EDPB's finding of infringement of Article 5(1)(a) fairness principle was similarly largely based on the lack of transparency, as regards the information that was presented to the data subject concerning the processing that would be carried out further to the Terms of Service.
 - iii. As already noted, the Transparency Decision imposed administrative fines totalling €225 million on WhatsApp arising from its failure to comply with its transparency obligations in the context of its Privacy Policy and related material. I have taken this previous sanction into account when proposing the fining range set out above so as to avoid the risk of punishing WhatsApp twice in respect of the same conduct. This factor necessitated a very significant reduction in the fine that might otherwise have been imposed, notwithstanding the significant turnover of the undertaking concerned and the outcome of the Article 83(2)(a) assessment, as recorded above.

WhatsApp's Final Submissions in response to the assessment of the Article 6(1) infringement for the purpose of Article 83(1), as introduced to this Decision following the adoption of the Article 65 Decision

9.64 WhatsApp, by way of its Final Submissions, disagreed with the above.

9.65 Addressing, firstly, WhatsApp's general (and repeated) submission that *"the reasoning in the Decision Extracts in respect of the calculation of the fine is inadequate, such that it is*

impossible to understand how the proposed fining range has been calculated or how the different factors discussed by the [Commission] have had an impact on the proposed fine.”⁹², I do not agree that this is the case. As is evident from the extensive analysis set out above, the Commission has clearly identified the factors that were considered relevant for the purpose of each of the individual Article 83(2) assessments. Furthermore, the manner in which the relevant factors have been taken into account, as a mitigating or aggravating factor, as well as the weight that has been attributed to each one has been clearly addressed. I have also identified the reasons why I consider the fining range proposed to satisfy the requirements of Article 83(1) GDPR.

9.66 The approach taken is in line with the Commission’s obligation to provide reasons for its decisions.

While the Commission is required to explain how it arrived at the level of a proposed fine, it is not required to apply such specificity so as to allow a controller or processor to make a precise mathematical calculation of the expected fine.⁹³

9.67 Turning to WhatsApp’s substantive submissions on the Article 83(1) assessment, I firstly note that it has submitted that the proposed fining range “is *inconsistent with the requirements of Article 83(1) GDPR*”⁹⁴ and that the fining range proposed “... *is excessive and higher than the minimum amount necessary to be “effective” and “dissuasive”, and therefore is not “proportionate”...*”.

9.68 In relation to the requirement for administrative fines to be **effective**, WhatsApp has restated¹⁹³ its view that the taking into account of “financial position” is an “error of law”. I note that I have already set out the reasons why I am required to take account of such matters as part of my assessment of the Article 83(2)(k) criterion, above. WhatsApp has further submitted⁹⁵ that, taking into account that it will be subject to a “potentially very onerous compliance order requiring significant expenditure of resources”, the imposition of an administrative fine is simply unnecessary to render this Decision effective. It has further submitted⁹⁶ that the imposition of a fine is not necessary or justified in circumstances where it has also made updates to its Terms of Service and Privacy Policy since the commencement of the Inquiry.

⁹² Final Submissions, paragraphs 10.2 and 11.2.

⁹³ See, by analogy, *HSBC Holdings plc and Others v Commission*, T-105/17, ECLI:EU:T:2019:675, paragraphs 336 – 354.

⁹⁴ Final Submissions, paragraph 11.1.¹⁹³

Final Submissions, paragraph 11.3

⁹⁵ Final Submissions, paragraph 11.4

⁹⁶ Final Submissions, paragraph 11.5

- 9.69 In response to the above, I note that the Commission is subject to a binding decision of the EDPB that requires the Commission to impose an administrative fine to address the finding of Article 6(1) (and taking into account the infringement of the Article 5(1)(a) principle of fairness), both of which were established by the Article 65 Decision. In the circumstances, it is simply not open to the Commission to disregard the clear instruction, in the Article 65 Decision, that requires the Commission to impose an administrative fine.
- 9.70 In relation to the requirement for administrative fines to be **dissuasive**, WhatsApp has submitted⁹⁷ that it relied on Article 6(1)(b) in good faith and, accordingly, there is no conduct that should be deterred. I note that this position is not consistent with views expressed by the EDPB in the Article 65 Decision and, accordingly, I am unable to take this submission into account. WhatsApp has further submitted that the order to bring processing into compliance will “inevitably have a significant dissuasive effect on WhatsApp and, to the extent relevant, any other controller undertaking similar processing”¹⁹⁷. As noted above, the purpose of an administrative fine is to sanction wrongdoing that it found to have occurred. This stands in contrast with measures such as an order to bring processing into compliance, which operates to bring about the required remedial action. In the circumstances, I do not consider the order that will be made pursuant to this Decision to be relevant, in the context of the requirement for the fining range proposed above to be dissuasive.
- 9.71 In relation to the requirement for administrative fines to be **proportionate**, WhatsApp has again restated⁹⁸ its position, as regards its good faith reliance on Article 6(1)(b) GDPR, and the entitlement of the Commission to take account of turnover when assessing the proposed fining range for the purpose of Article 83(1) GDPR. I have already addressed such matters further to the assessment of Article 83(2)(k) GDPR. While WhatsApp additionally submitted that no material gains were made in relation to the alleged infringement and that account should be taken of the fact that the WhatsApp service is free to users, I am not minded to take account of such matters in circumstances where there is no way for me to know, with certainty, what impact the infringement had on WhatsApp’s financial position. Furthermore, while I acknowledge that WhatsApp’s service is free to users, it is unclear how this is relevant to the Article 83(1) assessment.
- 9.72 In the circumstances, and having considered WhatsApp’s submissions on the matter, I remain of the view that the fining range proposed above satisfies the requirements of Article 83(1) GDPR.

⁹⁷ Final Submissions, paragraph 11.7 ¹⁹⁷

Final Submissions, paragraph 11.8

⁹⁸ Final Submissions, paragraphs 11.11 and 11.12

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

ASSESSMENT OF THE UNDERTAKING CONCERNED AND THE APPLICABLE FINING “CAP”

9.74 Having identified the range of the administrative fine that I consider to be effective, proportionate and dissuasive to the circumstances of the case, I must now identify the maximum limit of the fine that may be imposed so as to ensure that the Commission does not exceed this maximum when adopting its Decision. As already noted, the infringement of Article 6(1) GDPR is subject to the higher fining “cap” set out in Article 83(5) GDPR, as follows:

“Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

...”

9.75 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.”

9.76 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 financed⁹⁹”

9.77 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

⁹⁹ *Höfner and Elser v Macrotron GmbH* (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161 §21

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 infringement¹⁰⁰.

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

9.79 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 case¹⁰¹.

9.80 The CJEU has, however, established 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.

9.81 The CJEU has also established that,¹⁰² in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary¹⁰³.

9.82 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

¹⁰⁰ *Akzo Nobel and Others v Commission*, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, § 58 - 61

¹⁰¹ *Ori Martin and SLM v Commission* (C-490/15 P, judgment delivered 14 September 2016) ECLI:EU:C:2016:678 § 60

¹⁰² *Akzo Nobel and Others v Commission*, (C-97/08 P, judgment delivered 10 September 2009).

¹⁰³ Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, paragraph 48

its power to exercise a decisive influence over the conduct of its subsidiary¹⁰⁴. This reflects the position that:

“... the presumption of actual exercise of decisive influence is based, in essence, on the premise that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day business of that subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company ...”¹⁰⁵

- 9.83 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.
- 9.84 It is important to note that “decisive influence”, in this context, refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR, in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.

Application of the above to the within inquiry

- 9.85 Having reviewed the Directors’ Report and Financial Statements filed on behalf of WhatsApp with the Irish Companies Registration Office (in respect of the financial year ended 31 December 2021) I note that this document confirms, on page 3 thereof, that:

*“WhatsApp is a simple, reliable and secure messaging and calling application that is used by people and businesses around the world to communicate in a private way.
WhatsApp Ireland Limited is wholly owned by WhatsApp LLC, a company incorporated in*

¹⁰⁴ 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

¹⁰⁵ 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)

the United States of America. Its ultimate parent is Meta Platforms, Inc., (formerly Facebook, Inc.) a company incorporated in the United States of America.

The principal activity of the Company is acting as the data controller for European users of the WhatsApp service and the provision of services to WhatsApp LLC ...”

9.86 It is further confirmed, on page 5 thereof, that:

“Going concern

...The company’s ultimate parent undertaking, Meta Platforms, Inc., has indicated that it will provide such financial support to the Company, in the event that funds are not otherwise available, to enable it to meet its obligations as they fall due for a period of twelve months from the date of approval of the financial statements...”

9.87 It is further stated, on page 14 thereof, that:

“The ultimate holding company and ultimate controlling party is Meta Platforms, Inc., (formerly 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 Meta Platforms, Inc. The immediate parent company of the Company is WhatsApp LLC, a company established under the laws of the United States of America”

9.88 On the basis of the above, it appears that:

- a. WhatsApp is the wholly owned subsidiary of WhatsApp LLC.;
- b. WhatsApp LLC is ultimately owned and controlled by Meta Platforms Inc.; and
- c. As regards any intermediary companies in the corporate chain, between WhatsApp IE and Meta Platforms Inc., it is assumed, by reference to the statements recorded above, that the *“ultimate holding company and controlling party of the smallest and largest group of which [WhatsApp] is a member ... is Meta Platforms, Inc.”*

9.89 It follows, therefore, that:

- a. The corporate structure of the entities concerned and, in particular, the fact that Meta Platforms Inc. owns and controls WhatsApp LLC means that Meta Platforms Inc. is able to exercise decisive influence over WhatsApp’s behaviour on the market; and

- b. A rebuttable presumption arises that Meta Platforms Inc. does in fact exercise a decisive influence over the conduct of WhatsApp on the market.
- 9.90 If this presumption is not rebutted, it means that Meta Platforms Inc. and WhatsApp constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant fining “cap” for the purpose of Article 83(4) and 83(5) GDPR, would fall to be determined by reference to the turnover of the Meta Platforms Inc. group of companies.
- 9.91 The Commission put the above to WhatsApp, by way of letter dated 15 December 2022, and invited it to express its views, in relation to whether it agreed with the assessment set out above and, in particular, the rebuttable presumption set out at paragraph 9.89 above. In response, WhatsApp confirmed that:¹⁰⁶
- a. WhatsApp is the wholly owned subsidiary of WhatsApp LLC.; and
- b. WhatsApp LLC is ultimately owned and controlled by Meta Platforms Inc.
- 9.92 While WhatsApp furnished a range of submissions that disputed the above approach (as summarised below), it did not detail, by reference to the economic, organisational and legal links between the entities concerned why it regarded itself as being able to act independently on the market.
- 9.93 WhatsApp submitted that it is an error of law to apply the concepts of “turnover” and “undertaking”, from competition law, to the GDPR.¹⁰⁷ WhatsApp emphasised that the only explicit reference to competition law in the GDPR is found in Recital 150, which is in contrast with the position in competition law, where the explicit provision is made for the concept of an undertaking in Articles 101 and 102 TFEU.¹⁰⁸ WhatsApp submitted that the concept of an undertaking pierces the corporate veil in competition law, so as to impute responsibility to a parent company for infringements of its subsidiaries. WhatsApp placed particular reliance on the importance of the phrase “on the market”, and contrasts this with the position of data controllers under the GDPR, in circumstances where Article 4(7) GDPR explicitly states that controllers themselves determine the purposes and means of data processing, and in circumstances where the GDPR attributes liability to controllers.¹⁰⁹

¹⁰⁶ Letter dated 23 December 2022 from WhatsApp’s legal advisors to the Commission

¹⁰⁷ *Ibid*, page 2.

¹⁰⁸ *Ibid*, page 3.

¹⁰⁹ *Ibid*, pages 3-4.

²¹⁰ *Ibid*, page 4.

- 9.94 WhatsApp sought to draw particular attention to the fact that the substantive legal rules within the GDPR are addressed to controllers rather than the single economic unit, and that administrative orders are primarily directed at controllers, per Article 58 GDPR. Taking this into account, WhatsApp has submitted that “... *in determining whether separate legal entities ought to be treated as forming part of the same undertaking under the GDPR, the question is the extent to which the parent company can exert a dominant influence over the processing of personal data by the subsidiary.*”²¹⁰
- 9.95 I respectfully disagree with this suggestion, which appears to reduce the phrase “behaviour on the market”, which is the focus of the relevant assessment, in terms of parent’s ability to exercise influence, to a very limited position which concerns only the parent’s ability to influence its subsidiary’s data processing operations. Firstly, the approach proposed by WhatsApp (involving an assessment of where the decision-making power lies, in relation to the processing of personal data) is effectively a replication of the assessment that must be undertaken at the outset of the inquiry process, the outcome of which determines (i) the party/parties to which the inquiry should be addressed; and (ii) (in cross border processing cases) the supervisory authority with jurisdiction to conduct the inquiry. Given the consequences that flow from this type of assessment, it would not be appropriate for this assessment to be conducted at the decision-making stage of an inquiry.
- 9.96 Secondly, the suggested approach could not be applied equally in each and every case. Where, for example, the presumption of decisive influence has been raised in the context of a crossborder processing case where one of the entities under assessment is outside of the EU, an assessment of that entity’s ability to exercise decisive influence over the respondent’s data processing activities would likely exceed scope of Article 3 GDPR. Such a scenario risks undermining the Commission’s ability to comply with its obligation, pursuant to Article 83(1) GDPR, to ensure that the imposition of fines, in each individual case, is “effective, proportionate and dissuasive”.
- 9.97 Thirdly, the approach taken by the Commission does not exceed the territorial scope established by Article 3 GDPR. The personal involvement of any other entity in the alleged infringement is not a relevant consideration for the purpose of the required assessment. Accordingly, the assessment of whether or not any other entity is in a position to exercise decisive influence over the respondent’s behaviour on the market does not require the Commission to consider matters that might exceed the territorial scope of the GDPR.
- 9.98 Finally, the application of the approach that has been suggested by WhatsApp would be contrary to the clear intention of the legislature, as indicated by Recital 150 and the relevant *travaux préparatoires* (which are an accepted aid to interpretation, particularly

in relation to EU secondary legislation such as the GDPR). The suggested approach would represent a marked departure from the manner in which the required assessment is usually carried out. Accordingly, if this had been the intention of the legislature, it is unclear why this was not indicated in Article 83 GDPR or Recital 150 (either expressly, or by the incorporation of reference to the scoping provisions of Article 3 or to the concept of “main establishment”, as defined by Article 4(16), such that it is clear that the assessment of “behaviour on the market” should be limited to the processing of personal data in the EU).

9.99 Furthermore, the phrase “behaviour on the market” ought to be attributed the meaning normally ascribed to it in EU competition law. In summary, “behaviour on the market” describes how an entity behaves and conducts its affairs in the context of the economic activity in which it engages. Such behaviour will include matters such as the policies and procedures it implements, the marketing strategy it pursues, the terms and conditions attaching to any products or services it delivers, its pricing structures, etc. I therefore can see no basis in law, in WhatsApp’s submissions or otherwise, to deviate from this well-established principle as set out both in the GDPR, other provisions of EU law and the jurisprudence of the CJEU.

9.100 WhatsApp has also emphasised the fact that Articles 83(1)-(3) GDPR make no reference to the turnover of the undertaking. Specifically, it argues that:

“While reference is made in Article 83 to the turnover of the undertaking, this is limited to the provisions which govern the calculation of the fining caps; Articles 83(4)-(6). For the reasons set out above, [WhatsApp] does not accept that the language of Articles 83(4)-(6) imports the concept of the “undertaking”, as provided for in Articles 101 and 102 TFEU. However, even if it did (quod non), this concept is clearly not imported into the provisions which govern the calculation of the administrative fines to be imposed, namely, Articles 83(1)-(3) GDPR, which make no reference whatsoever to the turnover of the undertaking. It is submitted, therefore, that were the [Commission] to have regard to the turnover of [Meta Platforms Inc.] in calculating the administrative fine, this would constitute an error of law.”¹¹⁰

9.101 I note that I have already addressed this particular submission above, as part of the assessment of Article 83(2)(k) GDPR. As noted, the Commission is required by the EDPB’s Binding Decision 1/2021 to take account of the turnover of the undertaking concerned when calculating the quantum of the administrative fine to be imposed. I note that this position is further reflected in the EDPB’s Fining Guidelines 04/2022 (see, for example, paragraph 49 thereof).

¹¹⁰ *Ibid*, page 5.

9.102 For the avoidance of doubt, I note that there is a clear difference of opinion, between WhatsApp and the Commission, as regards the assessment of the relevant turnover, for the purpose of Article 83 GDPR and the function of that turnover, within Article 83 itself. I note that the Commission comprehensively addressed the position with WhatsApp previously, in the context of the WhatsApp Transparency Decision, and the Commission continues to rely on its position, as outlined therein (and as repeated above). Furthermore, the Commission notes that its approach is consistent with the position of the EDPB, as reflected in Binding Decision 1/2021 and Fining Guidelines 4/2022.

9.103 Applying the above to Article 83(5) GDPR, I firstly note 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. I note, in this regard, that Meta Platforms, Inc. reported the generation of revenue in the amount of \$117.929 billion for the year ending 31 December 2021.¹¹¹ The Commission understands this figure to correspond to the consolidated turnover of the group of companies headed by Meta Platforms, Inc. That being the case, the administrative fine imposed herein does not exceed the applicable fining “cap” prescribed by Article 83(5) GDPR.

SUMMARY OF THE ENVISAGED ACTION

9.104 I therefore decide to exercise the following corrective powers:

9.105 An order is hereby made, pursuant to Article 58(2)(d) GDPR, requiring WhatsApp to bring processing into compliance (“the **Order**”) within a period of six months commencing on the day following the date of service, in WhatsApp, of this Decision. The Order requires WhatsApp to take the necessary action to bring its processing of personal data for the purposes of service improvement and security features (excluding processing for the purpose of “IT Security” as defined by paragraph 90 of the Article 65 Decision) (“the **Processing**”) into compliance with Article 6(1) GDPR in accordance with the conclusion reached by the EDPB, as recorded at paragraphs 121 and 122 of the Article 65 Decision. More specifically, in this regard, WhatsApp is required to take the necessary action to address the EDPB’s finding that WhatsApp is not entitled to carry out the Processing on the basis of Article 6(1)(b) GDPR, taking into account the analysis and views expressed by the EDPB in Section 4.4.2 of the Article 65 Decision. Such action may include, but is not limited to, the identification of an appropriate alternative legal basis, in Article 6(1) GDPR, for the Processing together with the implementation of any necessary measures, as might be required to satisfy the conditionality associated with that/those alternative legal basis/bases.

¹¹¹ <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year2021-Results/default.aspx>.

9.106 An administrative fine is hereby imposed, pursuant to Articles 58(2)(i) and 83 GDPR, addressed to WhatsApp, in the amount of €5.5 million.

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

This Decision is addressed to:

**WhatsApp Ireland Limited 4
Grand Canal Square
Grand Canal Harbour
Dublin 2**

Dated the 12th day of January 2023

Decision-Maker for the Commission:

[sent electronically, without signature]

**Helen Dixon
Commissioner for Data Protection**

SCHEDULE 1

1 CHRONOLOGY, PROCEDURAL AND SCOPE MATTERS PERTAINING TO INQUIRY

1.1 The complaint (“the **Complaint**”) was lodged with the Hamburg Data Protection Authority: *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (“the **Hamburg DPA**”) on 25

May 2018 (the date on which the GDPR became applicable) by the Complainant’s representative (noyb – European center for digital rights) and was subsequently passed to the German Federal Data Protection Authority, the relevant national authority: *Bundesbeauftragter für den*

Datenschutz und die Informationsfreiheit (“the **German Federal DPA**”). The legal framework for the Complaint as lodged with the Commission is set out below. In brief, the Complaint concerns the lawfulness of WhatsApp Ireland Limited’s (“**WhatsApp**”) processing of personal data, specifically data processing on foot of the Complainant’s acceptance of its Terms of Service (and purportedly her acceptance of its Privacy Policy), and the transparency of information provided by WhatsApp to the Complainant about that processing.

- 1.2 The Commission began the inquiry (“the **Inquiry**”) by designating an investigator (“the **Investigator**”), who produced a draft of an inquiry report (“the **Draft Inquiry Report**”) and, following submissions from the WhatsApp and the Complainant’s representative, a final inquiry report (“the **Final Inquiry Report**”). In considering this Inquiry, I have relied on the facts as set out in the Final Inquiry Report. I have also had regard to the views set out by the Investigator in the Final Inquiry Report, as well as to the entirety of the file, in preparing this Schedule 1.
- 1.3 The preliminary draft decision (“the **Preliminary Draft**”) set out my provisional findings, as the decision-maker in this matter, in relation to (i) whether or not an infringement of the GDPR has occurred/is occurring, and (ii) the envisaged action, if any, to be taken by the Commission in respect of same. The Preliminary Draft Decision and a draft of this Schedule 1 were provided to WhatsApp and the Complainant’s representative for the purpose of allowing them to make submissions on my provisional findings.
- 1.4 The submissions of WhatsApp were received and taken into account by the Commission. In relation to the Complainant’s representative, no submissions were received and the Commission therefore wrote to the Complainant’s representative’s legal advisors by letter dated 25 February 2022. In that letter, the Commission indicated that if no reply were received, the Commission would operate on the basis that the Complainant’s representative did not wish to make submissions. In the alternative, the Commission proposed that the Complainant’s representative was free, if it wished, to rely on submissions it made in a factually and legally similar complaint into the Facebook platform (with internal Commission inquiry reference IN 18-5-5). This was in circumstances where the Complainant’s representative had elected to do this in relation to a factually and legally similar complaint into the Instagram platform (bearing internal Commission inquiry reference IN 18-5-7). No further correspondence was received, and the Commission has therefore proceeded on the basis that the Complainant’s representative does not wish to make submissions in relation to the Preliminary Draft.

- 1.5 Having taken careful account of those submissions, I finalised a draft decision (“the **Draft Decision**”) and associated updated draft of this Schedule 1. As the cross-border

processing under examination in this Inquiry was such that all other EU/EEA supervisory authorities (the “SAs”, each one being an “SA”) were engaged as supervisory authorities concerned (“the CSAs”) for the purpose of the cooperation process outlined in Article 60 GDPR. Following the circulation of the Draft Decision and Schedule to the CSAs for the purpose of enabling them to express their views, in accordance with Article 60(3) GDPR, objections were raised by the SAs of France, Germany (Federal, and representing a co-ordinated response by the German SAs), Finland, Italy, the Netherlands and Norway. A number of comments were also exchanged by various CSAs.

- 1.6 Having considered the matters raised, the Commission, by way of a composite response memorandum dated 1 July 2022, set out its responses together with the compromise positions that it proposed to take in response to the various objections and comments. Ultimately, it was not possible to reach consensus with the CSAs on the subject-matter of the objections and, accordingly, the Commission determined that it would not follow them. That being the case, the Commission referred the objections to the European Data Protection Board (the “EDPB” or the “Board”) for determination pursuant to the dispute resolution mechanism provided for in Article 65(1)(a) GDPR. In advance of doing so, the Commission invited WhatsApp to exercise its right to be heard in respect of the objections (and comments) that the Commission proposed to refer to the EDPB, along with the Commission’s composite response memorandum dated 1 July 2022, and the communications received from the CSAs in reply to the Composite Response.
- 1.7 WhatsApp exercised its right to be heard by way of its submissions dated 17 August 2022 (“the **Article 65 Submissions**”). The EDPB adopted its decision pursuant to Article 65(2) GDPR (“the **Article 65 Decision**”)¹¹² on 5 December 2022 and notified it to the Commission and CSAs on 15 December 2022. As set out in Article 65(1) GDPR, the Article 65 Decision is binding on the Commission. Accordingly, and as required by Article 65(6) GDPR, the Commission has now amended its Draft Decision, by way of this final decision (“the **Decision**”), in order to take account of the EDPB’s determination of the various objections from the CSAs which it determined to be “relevant and reasoned” for the purpose of Article 4(24) GDPR. Following the amendment of the Draft Decision to take account of the EDPB’s Article 65 Decision, WhatsApp was invited to exercise its right to be heard in relation to those aspects of the Draft Decision, in relation to which the Commission was required to make a final determination or, otherwise, to exercise its discretion. WhatsApp furnished its submissions on these matters under cover of letter dated 23 December 2022 (“the **Final Submissions**”).

¹¹² Binding Decision 5/2022 on the dispute submitted by the Irish SA on WhatsApp Ireland Limited, adopted 5 December 2022.

- 1.8 For the avoidance of doubt, this Schedule is an integral and operative part of the Decision for the purposes of Article 60 and 65 GDPR. The previous division of material into two documents was entirely a structural choice, so as to enable a more exclusive focus on the substantive Complaint in the main document, while dealing with matters of a more procedural nature herein. It has been incorporated into the Decision itself as part of the finalisation process, prior to adoption.

LEGAL BASIS FOR THE INQUIRY

- 1.9 The Inquiry in this case was conducted by the Investigator under Section 110 of the Data Protection Act 2018 Act (the “**2018 Act**”).
- 1.10 The decision-making process for the Inquiry which applies to this case is provided for under Section 113(2)(a) of the 2018 Act. Additionally, Section 113(3)(a) of the Act requires that the Commission must consider the information obtained during the Inquiry; decide whether an infringement is occurring or has occurred; and if so, decide on the envisaged action (if any) to be taken in relation to the data controller. This function is performed by me in my role as the decision-maker. In so doing, I have carried out an independent assessment of all of the materials provided to me by the Investigator.
- 1.11 As stated above, the Inquiry was commenced pursuant to Section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the Commission has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.
- 1.12 In his consideration of the material, the Investigator was satisfied that WhatsApp constitutes a data controller and that the processing referred to in the Complaint constitutes cross-border processing, such that the Commission is the lead supervisory authority as set out in the GDPR. I my decision in this regard below.

REFERRAL BY GERMAN FEDERAL DPA

- 1.13 The Complaint was referred to the Commission by the German Federal DPA on the basis that (i) the Complaint concerns cross-border processing and (ii) WhatsApp, as the data controller, has its main establishment in Ireland. In this regard, the German Federal DPA forwarded the Complaint to the Commission on 31 May 2018. The Commission assessed the Complaint as lead supervisory authority, commenced the Inquiry under Section 110 of the 2018 Act on 20 August 2018. WhatsApp and the Complainant’s representative were also notified of the commencement of the Inquiry on 20 August 2018.

STATUS OF THE COMPLAINANT'S REPRESENTATIVE

1.14 The Complainant's representative is acting as a representative of a named individual in accordance with Article 80 GDPR, which states that:

"The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf..."

1.15 For the purposes of assessing compliance with Article 80 GDPR, it is necessary to assess whether the Complainant's representative was a properly constituted not-for-profit body with objectives in the public interest and that was actively engaged in "the field of the protection of data subject rights". In this regard, the Investigator consulted the Complainant's representative's website, and its articles of association, which explain that it is a "verein" (association) under Austrian law. Having reviewed paragraphs 101-106 of the Final Inquiry Report and Appendix 4 of the Final Inquiry Report (the Complainant's representative's articles of association), I am satisfied that the Complainant's representative meets the definition set out in Article 80 GDPR. The Complainant's representative is a not-for-profit body that appears on its face (although the Commission has no specific competence to rule in this regard) to be validly constituted in accordance with Austrian law, with objectives which are in the public interest. From having reviewed this information, I am also satisfied that the Complainant's representative is active in the field of the protection of data subject rights. On this basis, I am satisfied that these all meet the definition in Article 80 GDPR.

1.16 Moreover, it is necessary to determine the validity of the data subject's mandate in order to decide whether the Complainant's representative may represent them. I am satisfied, having reviewed paragraphs 107-112 of the Final Inquiry Report and Appendix 6 of the Final Inquiry Report (the data subject's "mandate") that the mandate provided to the Complainant's representative by the data subject was lawful, and that therefore the Complainant's representative has the right to represent the data subject in this matter. The mandate includes the name, address and signature of the data subject being represented by the Complainant's representative. I note, as was noted by the Investigator, that the mandate specifically refers to "forced consent to the update privacy policy that I clicked on to in May 2018". On an objective reading of this mandate, the Complainant's representative was given authority to represent the data subject in relation to alleged infringements of the GDPR concerning agreement to the Terms of Service and Data Policy.

1.17 Subsequent documents have also been provided by the Complainant's representative in order to argue that it is not limited in any way in its representation of the Complainant. The law is clear that such documentation cannot alter, *post hoc*, the nature of the data subject mandate that was

provided to the Complainant's representative in accordance with Article 80 GDPR to launch a complaint on its behalf. The nature of the Complaint was specified and detailed in the mandate. However, as the scope of the Complaint as I find below does not, in my view, conflict with the mandate, the question of whether any additional documentation can subsequently broaden the scope of the Complainant's representative's mandate in relation to an extant inquiry procedure is moot.

1.18 WhatsApp expressed no particular view on the Complainant's representative's status under Article 80 GDPR, or on the data subject's mandate, save in respect of its position on the scope of the Inquiry. WhatsApp has argued that the scope of the Inquiry as determined by the Commission was too broad both because it goes beyond, in WhatsApp's view, the text of the Complaint, and because it goes beyond the scope of the data subject's mandate.¹¹³ I consider this argument below when I consider the general question of the scope of the Inquiry.

PROCEDURAL CONDUCT OF INQUIRY

1.19 As set out above, the Inquiry was commenced on 20 August 2018 for the purposes of examining and assessing the circumstances surrounding the Complaint as referred to the Commission by the German Federal DPA, with a view to ultimately facilitating a decision under Section 113(2)(a) of the Act.

1.20 The Commission commenced the Inquiry as it was "*... of the opinion that one or more provisions of the [2018] Act and/or the GDPR may have been contravened in relation to the personal data of the data subject who is represented by the Complainant pursuant to Art. 80(1) GDPR...*"²¹⁵ The Commission formed this view on the basis of the contents of the Complaint and the arguments it sets out. WhatsApp and the Complainant's representative were informed of the commencement of the Inquiry by way of a letter dated 20 August 2018. The letter to WhatsApp set out that the scope of the Inquiry would encompass the contents of the Complaint. The letter also set out a number of queries for WhatsApp.

1.21 The Investigator subsequently wrote to WhatsApp on 4 February 2019 setting out the alleged infringements in the Complaint and seeking WhatsApp's submissions on specific matters. WhatsApp responded to these queries, and the preliminary queries contained in the letter to WhatsApp dated 20 August 2018, by way of correspondence and attached submissions on 11 March 2019.

1.22 Meanwhile, a number of procedural issues were raised by the Complainant's representative in correspondence dated 3 December 2018. These issues consisted of an allegation of delay on the part of the Commission, and an allegation of bias on the part of the Commission, and a rejection of

¹¹³ WhatsApp submissions on Preliminary Draft, paragraph 4.3.

²¹⁵ Letter from the Commission to WhatsApp, 20 August 2018.

the interpretation of the Complainant's scope proposed by the Investigator. The Investigator responded to the Complainant's representative on 16 January 2019 refuting the allegations in strong terms. A further phone call took place between the Investigator and Mr. Maximilian Schrems, honorary chairman of noyb – European center for digital rights, i.e. the Complainant's representative, on 25 January 2019, in this regard.

- 1.23 The Complainant's representative sent a letter to the Investigator dated 29 February 2019, raising a number of additional procedural concerns including a query as to the nature of the procedure being utilised by the Commission, as well as concerns and queries surrounding the exchange of documents. The Investigator responded to these queries by way of letter dated 28 March 2019.
- 1.24 Mr. Maximilian Schrems raised a number of these concerns with the Investigator in a phone conversation on 1 April 2019. Further to this, the Complainant's representative wrote to the Investigator on 19 April 2019 to set out the concerns in writing. These concerns related to dealing directly with the Commission in circumstances where the Complaint was lodged with the German Federal DPA, as well as concerns surrounding the applicability of Irish procedural law as opposed to German procedural law, and conflicts between Irish procedural law and German procedural law. These concerns were also raised by the Complainant's representative in its submissions on the Draft Inquiry Report and were addressed in the Final Inquiry Report. I address these concerns and procedural issues below.
- 1.25 Further correspondence was sent to the Investigator by both the Complainant's representative and the Complainant's representative's legal representative on 24 February 2020, expressing concerns regarding, *inter alia*, the impact of a draft inquiry report in a separate but similar inquiry opened by the Commission on foot of a separate but similar complaint, where the Complainant's representative was also representing that complainant. The letter made further allegations relating to delay and a failure to provide the Complainant's representative with sufficient documentation, and threatened to take legal proceedings against the Commission unless these grievances were addressed.
- 1.26 The Investigator wrote to the Complainant's representative's solicitors on 23 March 2020, setting out that it was not appropriate that further submissions would be made in the herein Inquiry at that point, and that any concerns the Complainant's representative had could be set out comprehensively when it had an opportunity to make submissions on the Draft Inquiry Report, which was still being prepared. The Investigator also responded to and refuted, in that correspondence, allegations relating to the Commission's procedures, including that they were, *inter alia*, "unwieldy". The Investigator set out that all necessary documentation had been provided to the Complainant's representative.
- 1.27 Having completed the Draft Inquiry Report, the Investigator furnished WhatsApp and the Complainant's representative with a copy of it on 20 May 2020. WhatsApp's submissions on the Draft Inquiry Report were received by the Investigator on 22 June 2020.

1.28 The Complainant's representative's submissions on the Draft Inquiry Report, which were delayed due to issues of translation, are dated 4 September 2020.

1.29 In terms of its contents, the Final Inquiry Report sets out the factual background, and the scope and legal basis, for the Inquiry. It also provides an outline of the facts as established during the course of the Inquiry, an outline of the dispute about the scope of the Inquiry and the Investigator's view on same, and an outline of the procedural disputes that arose during the Inquiry and the Investigator's view on same. The Final Inquiry Report further sets out the Investigator's views as to whether, in respect of these matters, WhatsApp complied with its obligations under GDPR and the 2018 Act.

2 Procedural Issues Decided

2.1 As set out above, this is a schedule to, and integral part of, the Decision, (at this point, I note that I am the sole member of the Commission) in accordance with Section 113 of the 2018 Act. Section 113 of the 2018 Act provides as follows:

(2) Where section 109 (4)(a) applies, the Commission shall—

(a) in accordance with subsection (3), make a draft decision in respect of the complaint (or, as the case may be, part of the complaint) and, where applicable, as to the envisaged action to be taken in relation to the controller or processor concerned, and

(b) in accordance with Article 60 and, where appropriate, Article 65, adopt its decision in respect of the complaint or, as the case may be, part of the complaint.

(3) In making a draft decision under subsection (2)(a), the Commission shall, where applicable, have regard to—

(a) the information obtained by the Commission in its examination of the complaint, including, where an inquiry has been conducted in respect of the complaint, the information obtained in the inquiry, and

(b) any draft for a decision that is submitted to the Commission by a supervisory authority in accordance with Article 56(4).

(4) Where the Commission adopts a decision under subsection (2)(b) to the effect that an infringement by the controller or processor concerned has occurred or is occurring, it shall, in addition, make a decision—

(a) where an inquiry has been conducted in respect of the complaint-

- (i) *as to whether a corrective power should be exercised in respect of the controller or processor concerned, and*
- (ii) *where it decides to so exercise a corrective power, the corrective power that is to be exercised,*

- 2.2 In accordance with Section 113, it is for me, as the sole member of the Commission, to consider the information obtained in the course of the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the envisaged action in respect of the controller (if any). In so doing, I will carry out an independent assessment of all of the materials provided to me by the Investigator.
- 2.3 Given that the Commission is the lead supervisory authority under Article 56(1) GDPR for the purposes of the data processing operations at issue, I am obliged under Section 113(2) and Article 60(3) GDPR to complete a draft decision to be provided to any supervisory authorities concerned, as defined in Article 4(22) GDPR.
- 2.4 As set out above at paragraph 1.1, this concerns my Decision, having submitted the Draft Decision under Article 60(3) GDPR to the CSAs, and having taken account of the Article 65 Decision, as explained in the text of the Decision itself. The purpose of the Draft Schedule and the Preliminary Draft Decision were to allow the parties to make any submissions in respect of my provisional findings set out. This is the finalised version of the Decision (incorporating the previous schedule), as also explained in further detail in the Decision.

DECISION-MAKING PROCESS – MATERIALS CONSIDERED

- 2.5 The Final Inquiry Report was transmitted to me on 18 January 2021, together with the Investigator’s file, containing copies of all correspondence exchanged between the Investigator, WhatsApp and the Complainant’s representative; and copies of any submissions made by WhatsApp and the Complainant’s representative, including the submissions made by them in respect of the Investigator’s Draft Inquiry Report. A letter then issued to both WhatsApp and the Complainant’s representative on 6 April 2020, to confirm the commencement of the decision-making process. For the avoidance of doubt, I have had regard to all material contained in the file when preparing this Decision.
- 2.6 As decision-maker, I must be satisfied that WhatsApp is a controller within the meaning of the GDPR, that the Commission has competence in respect of this Inquiry, and that fair procedures have been followed throughout the Inquiry. As I have set out above, a number of procedural complaints were made by the Complainant’s representative throughout the Inquiry process. These issues are addressed in this Schedule 1.

WHATSAPP AS CONTROLLER

2.7 In commencing the Inquiry, the Investigator was satisfied that WhatsApp is the controller, within the meaning of Article 4(7) of the GDPR, in respect of the personal data that was the subject of the Complaint. In this regard, WhatsApp confirmed that it was the controller for data processing in the European Union in a letter to the Investigator dated 11 March 2019, where it stated that it was responsible for:

- “• Making the Service available to EU users;*
- Setting policies governing how EU user data is processed;*
 - Controlling access to and use of EU user data;*
 - Handling and resolving data-related inquiries and complaints from EU users of the Service whether directly or indirectly via regulators;*
 - 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.”*

2.8 The concept of controllership is defined in Article 4(7) GDPR which states that a controller is

“... the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”.

2.9 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 in part in relation to 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.

2.10 In relation to the work of the Commission, and my work as Commissioner, it is clear to me based on direct experience that decisions in relation to the purposes and means of data processing for European data subjects are made by WhatsApp Ireland Limited. By way of

recent example, a largescale own-volition inquiry was conducted by the Commission into the transparency of WhatsApp's Privacy Policy, and a number of orders to bring the Privacy Policy into compliance were made.¹¹⁴ It is clear to the Commission from this engagement that WhatsApp Ireland Limited exercises the role of data controller in this regard. Moreover, in the context of the dispute resolution procedure pursuant to Article 65 GDPR that was triggered in that same inquiry, the concerned supervisory authorities and European Data Protection Board ("the **EDPB**") did not contest the Commission's position, in this regard.

COMPETENCE OF THE COMMISSION

2.11 Pursuant to Article 56(1) GDPR, "*... the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor*". It follows that the Commission is only competent to act as the lead supervisory authority if (i) WhatsApp's main or single establishment in the Union is located in Ireland, and (ii) there is cross-border processing as defined in the GDPR.

2.12 As regards the requirement that, in order to come within the competence 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.

2.13 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. 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.

2.14 WhatsApp confirmed to the Commission, in the course of the Inquiry, that it regarded the above position to be the case.¹¹⁵ In this regard, I further note that the Investigator, and the Commission generally, was satisfied, in commencing the Inquiry, that WhatsApp Ireland Limited was the main establishment in the European Union within the meaning of Article 56(1) GDPR. Moreover, I have

¹¹⁴ https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-0921_en.pdf.

¹¹⁵ Final Inquiry Report, paragraph 99.

already found, for the reasons set out above, that decisions on the purposes and means of the processing of personal data are taken by WhatsApp Ireland Limited. For these reasons and the reasons already set out above, I am satisfied that WhatsApp Ireland Limited is WhatsApp's place of central administration in the Union. I am also satisfied, on the information available to me, that decisions which relate to the means and purposes of data processing are made by WhatsApp Ireland.

2.15 Turning to cross-border processing, cross-border processing is defined in Article 4(23) GDPR as either:

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

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

2.16 I note that the Investigator was satisfied that there was cross-border processing carried out by WhatsApp (within the meaning of Article 4(23) GDPR), in relation to the personal data that was the subject of the Complaint.¹¹⁶ Given the scale of WhatsApp's operations across the European Union outlined above, I am satisfied that there is cross-border processing as defined in the GDPR for the purposes of this Complaint. This position of the Commission has been acknowledged by WhatsApp.¹¹⁷

2.17 I am satisfied based on the above evidence secured through publicly available sources, information voluntarily provided by WhatsApp, and information acquired by the Commission in the course of conducting investigations, that WhatsApp Ireland is the data controller for EU users and is the organisation's place of central administration in the Union. I am also satisfied, for the reasons set out above, that this Complaint concerns cross-border processing. I therefore agree with the Investigator that WhatsApp Ireland meets the definition of “main establishment” in Article 4(16) GDPR, and that therefore the Commission is competent to act as lead supervisory authority in accordance with Article 56 GDPR.

CONSUMER PROTECTION AND COMPETITION AUTHORITIES

2.18 The Investigator informed the Complainant's representative by letter dated 16 January 2019 that the Commission does not have competence to investigate matters pertaining to competition or consumer

¹¹⁶ *Ibid.*

¹¹⁷ WhatsApp submissions on Preliminary Draft, paragraph 3.1.

law.¹¹⁸ Therefore, the Investigator provided the relevant competition¹¹⁹ and consumer¹²⁰ law authorities with a partially redacted copy of the Complaint for consideration of matters which may fall within their competence.

2.19 In submissions on the Draft Inquiry Report, the Complainant's representative expressed "*amazement*" that the Commission had referred matters relating to competition and consumer law to the relevant regulatory authorities.¹²¹ The Complainant's representative submitted that the referral to other regulatory authorities was not appropriate as the Commission had competence to consider the entirety of the Complaint.¹²²

2.20 In this regard, I emphasise that the Commission's competence is limited to matters pertaining to data protection. Accordingly, the Commission cannot consider issues which relate to competition or consumer law. Therefore, I am satisfied that the Investigator was correct in referring the appropriate matters to the relevant authorities.

THE RIGHT TO BE HEARD AND ACCESS TO THE FILE

2.21 In the course of the Inquiry, the Complainant's representative also submitted that "*... both parties have to receive all files, documents and submissions before a DPA to be able to defend their legal positions*".¹²³ In response to the Complainant's representative's request for access to the complete file, the Investigator correctly informed the Complainant's representative, by way of letter dated 16 January 2019, that "*... there is no statutory right of access to the complete inquiry file under Irish law*" and that the parties to the Complaint would be provided with the material information and documents as appropriate to ensure the right to be heard.²²⁶ I agree with the Investigator on this issue and do not propose to consider it further.

ISSUES OF GERMAN LAW

2.22 The next procedural issue is an overarching point that is relevant to each of the other individual points raised by the Complainant's representative, and so I will consider this point before considering

¹¹⁸ Letter from the Commission to the Complainant's representative dated 16 January 2019, at p. 5.

¹¹⁹ The Irish Competition and Consumer Protection Commission (CCPC), Belgian Competition Authority, and the European Commission Directorate General for Competition (DG COMP).

¹²⁰ Irish Competition and Consumer Protection Commission (CCPC), Consumer Protection Division of the Belgian Federal Public Service Economy, S.M.E.s, Self-employed and Energy, and the European Commission Directorate General for Justice and Consumers (DG JUST).

¹²¹ Complainant's representative's submissions on Draft Inquiry Report, paragraph 2.7.

¹²² *Ibid.*

¹²³ Letter from the Complainant's representative to the Commission dated 3 December 2018, at p. 3.

²²⁶ Letter from the Commission to the Complainant's representative dated 16 January 2019, at p. 5.

the other points in turn. This Complaint was lodged with the Hamburg SA, and was then transferred by the German Federal SA to the Commission as lead supervisory authority in accordance with Article 56 GDPR. The Commission then launched a statutory inquiry in accordance with Irish law. The Complainant's representative, however, argues that because the Complaint itself was lodged with the Hamburg SA in Germany, the Complaint must be handled in accordance with the procedural laws of both Germany and Ireland.

2.23 The Complainant's representative made these arguments in its submissions to the Investigator,¹²⁴ and specifically argues that the applicable procedural law is the *Verwaltungsverfahrensgesetz* ("the **VwVfG**"), Germany's code of administrative procedure. It is the Complainant's representative's view that the VwVfG permits the alteration of the scope of a procedure in particular circumstances while the Inquiry is ongoing, and seeks to rely on this in order to dispute the Investigator's view of the scope of the Complaint, and to alter that scope and/or to ensure that "*the substantive request is now adapted accordingly*".¹²⁵ My decision on scope of the Complaint is considered in detail below, and at this point I am solely considering the applicability or otherwise of the VwVfG to the actions of the Commission in general.

2.24 As the decision-maker at the Commission, I take no view on the Complainant's representative's characterisation of the VwVfG or of any other questions of German law. The Commission was established in Ireland by the 2018 Act, thereby meeting Ireland's obligations to establish such an authority under Article 51 (and Chapter VI generally) GDPR, given it is directly applicable in Ireland pursuant to Article 288 of the Treaty on the Functioning of the European Union. Section 12 of the 2018 Act provides a number of functions for the Commission "*... in addition to the functions assigned to the Commission by virtue of its being the supervisory authority for the purposes of the Data Protection Regulation*".

2.25 Chapter VI of the GDPR set out in detail the responsibilities and powers of supervisory authorities. While it is not necessary to set out Chapter VI here, it is noteworthy that Article 51(1) GDPR states that "*... [e]ach Member States shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation*" [my emphasis]. Moreover, Section 12 of the 2018 Act does not confer any powers on the Commission in respect to the laws of any other jurisdiction.

2.26 The powers of the Commission must be limited to those conferred on it by law. The Commission is tasked with encouraging, monitoring and enforcing compliance with the GDPR. In that context it is, like all other public authorities in the State, bound by the administrative law of Ireland and EU law, including EU law on fair procedures and the European Charter of Fundamental Rights and Freedoms. Further, as I stated above, Article 56(1) GDPR sets out that "*... the supervisory authority of the main*

¹²⁴ Complainant's representative's submissions on Draft Inquiry Report, *inter alia*, paragraph 2.1.

¹²⁵ *Ibid.*

establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority”.

2.27 The Commission therefore derives its legal authority to handle the Complaint from the GDPR and the 2018 Act, and is, in that regard, bound by the legal order set out above. The Commission is not bound, nor must it have regard to, the administrative law of Germany, or of any other jurisdiction. Moreover, it seems to me that not only does the administrative law of Germany not bind the Commission, but that any attempt by the Commission to apply such law would be plainly *ultra vires* the powers conferred on the Commission by law. WhatsApp has made no particular submission on this issue in response to the Preliminary Draft.

ALLEGATION OF BIAS

2.28 As has been set out above, the Complainant’s representative wrote to the Investigator on 3 December 2018 raising a number of procedural issues, including an allegation of bias on the part of the Commission, which I will address here. I will subsequently address the Complainant’s representative’s allegation that the manner in which the Commission dealt with the scope of the Complaint was contrary to its right to fair procedures, before considering the substantive question of the scope of the Complaint in the subsequent section.

2.29 In the letter dated 3 December 2018, the Complainant’s representative alleged that there had been prior “approval” by the Commission of the legal bases used by Facebook Ireland Limited, now known as Meta Platforms Ireland Limited (“**Facebook**”), a member of the same family of companies as WhatsApp, for processing personal data. This was based in part on a statement made in Vienna’s *Landesgericht* (Regional Court) that the “... *used legal basis for the processing of data under GDPR was developed under extended regulatory involvement by the [Commission] in multiple personal meetings between November 2017 and July 2018*”.¹²⁶ In the letter, the Complainant’s representative stated that “... [t]his does not just raise questions about your claim that you have to “investigate” and “inquire” [sic.] this matter – when in fact you have already negotiated with the Facebook Group about these legal and factual questions between 2017 and 2018, but raises issues about an obvious bias of a decision maker that has previously approved the criticized mechanism.”¹²⁷

2.30 In the same letter, the Complainant’s representative referred to the existence of a rule against bias in both Ireland other jurisdictions, but did not elaborate on its legal views of the nature of the test in either jurisdiction, and did not present any arguments explaining why, in its view, the Commission had acted in a manner that contravened any such test. Moreover, the Complainant’s representative offered no evidence to substantiate the factually inaccurate claim that the Commission “previously

¹²⁶ Case 3Cg52/14k at the LGfZRS Wien, paragraph 209.

¹²⁷ Letter from Complainant’s representative to Commission, 3 December 2018.

approved” the “mechanism” in question or to substantiate the allegation that the consultation process gave rise to the apprehension of bias.

2.31 The Investigator responded to this and other allegations in a letter dated 16 January 2019. The Investigator correctly observed that the allegations of bias were unsubstantiated, and confirmed that “... [the Commission] *does not and never has, endorsed, jointly developed, approved or in any other way assented or consented to a controller’s or processor’s policies or position in relation to compliance with its data protection obligations.*” It was clarified that the interactions referred to by Complainant’s representative were for the purpose of “... *being updated...and being providing high level feedback*” to both Facebook and to a large number of other private and public sector organisations with which the Commission interacts as part of its “... *consultation and engagement with regulatory stakeholders.*” I agree with the Investigator’s view just set out, for the reasons which I have set out above. I also note that while the consultation process being objected to related to Facebook, the Complainant’s representative raised this issue of bias in relation to the herein Inquiry as well.

2.32 I also note and agree with the Investigator’s statement in the same letter that outlined the Commission’s statutory obligations under the Data Protection Acts 1988 and 2003, which were in force at the time. This also applies, as was pointed out by the Investigator, under Article 57 GDPR. The Commission implements these obligations to promote awareness of data protection law by maintaining an active consultation function. The Investigator also clarified that the Commission “... *makes it abundantly clear to any organisation that seeks to consult with it that this is the premise upon which consultation takes place and that it is entirely a matter for that organisation to ensure that it is in compliance with data protection law.*” This is, in my view, an accurate characterisation of the position. In a subsequent telephone call with staff of the Commission on 25 January 2019, Mr. Maximilian Schrems, raised the matter of bias once again. At this point, a Deputy Commissioner at the Commission reiterated the Commission’s position, in this regard, to Mr. Schrems.¹²⁸

2.33 This issue of bias was not raised again until the Complainant’s representative furnished the Investigator with submissions on the Draft Inquiry Report dated 4 September 2020. For the sake of completeness, the entirety of the Complainant’s representative’s submission, in this regard, is set out below:

“In another case against Facebook it became apparent that concerning the procedure criticised here, i.e. the lawfulness of the processing, Facebook and the [the Commission] have worked together in ten sessions. This is evident, among other things, on page 2 of the pleading of 27.9.2018 by Facebook in that procedure (Appendix A). That is why we draw attention to the problem of partiality.

It seems difficult to imagine that the authority can make use of its power to impose sanctions if it has worked out in advance the criminal procedure with (the) Facebook (group) to which

¹²⁸ Memorandum of phone call, 25 January 2019.

WhatsApp belongs. This also results in a potential contradiction with the GDPR, which provides for "effective, proportionate and dissuasive" fines in Article 83(1).

We do not yet know how the Irish authority wants to deal with this problem and we expressly reserve for ourselves remedies for this."¹²⁹

2.34 As is evident from this quotation, the Complainant's representative offered no specific evidence in respect of this unsubstantiated allegation. Moreover, no reference is made to the Commission's clarification that no approval or authorisation for the Terms of Service was provided to WhatsApp (or Facebook) by the Commission. The premise of the Complainant's representative's argument, as had already been pointed out by the Investigator, is incorrect. The reference to "meetings" in Facebook's submissions cited by the Complainant's representative in the above quotation is the only reference to the Commission's consultation function in any submissions made by Facebook in the inquiry in question, and indeed does not relate to WhatsApp, or to this Inquiry. The reference is as follows:

"We have drafted this response against the background of our detailed direct engagement with the Commission prior to the implementation of the recent update to our terms, spanning 10 meetings, which covered many of the issues responded to herein. Facebook Ireland has not materially changed its compliance approach since these meetings."

2.35 I moreover note, in this regard, that while Facebook, Inc. was WhatsApp's and Facebook's parent company at the time, and that they were therefore both part of the "Facebook family of companies", WhatsApp is an entirely separate company from Facebook, and was not involved in the said consultation process referred to by Facebook and the Complainant's representative.

2.36 It is clear that this is a reference to a consultative process, and at no point does WhatsApp or its parent, Facebook, assert that the Terms of Service were approved or endorsed by the Commission; it is merely asserted that these Terms of Service have not changed since a consultation process took place. A controller would of course not be entitled to rely on remarks made in such meetings. In addition, it is not clear to me how WhatsApp can be said to be using the above statement to support its legal position, or indeed any argument, in relation to the Inquiry, particularly in circumstances where it relates to an entirely different data controller. For the purpose of providing additional context, I also emphasise that this quotation is taken from a two-page covering letter preceding submissions to the Commission in the context of a separate inquiry, as opposed to being extracted from such submissions to the Commission or being part of any submissions made in the herein Inquiry.

2.37 Finally, this matter was raised, indirectly, in the form of an "open letter" published by the Complainant's representative and sent to other SAs and to the EDPB. In this letter, public allegations were made about the Commission's cooperation with what the Complainant's representative called

¹²⁹ Submissions of Complainant's representative on Draft Inquiry Report, paragraph 2.8.

Facebook’s “consent bypass”.¹³⁰ To the extent that this letter directly addresses the allegation of bias at all, it once again proceeds on the false factual premise that that WhatsApp (and Meta/Facebook companies generally) “... *simply followed the [Commission]’s advice.*” It is further alleged that this renders the Commission’s processes “... *structurally biased because it is essentially reviewing its own legal advice.*” It has already been clarified above that, contrary to this assertion, the Commission did not approve any such mechanism, nor did it provide legal advice to Facebook/WhatsApp, or any other data controller. It has also been clarified that WhatsApp has in fact not sought to rely on such consultations in this Inquiry.

2.38 In the open letter, it was alleged that “... [k]eeping these meetings confidential is only adding to the impression that the [Commission] and Facebook have engaged in a relationship that is inappropriate for a neutral and independent oversight authority.”¹³¹ Aside from the fact that the Commission’s consultation function is widely publicised, such an allegation has no basis in law. The relevant facts have been provided to the Complainant’s representative by the Commission on multiple occasions, and a reasonable and objective explanation of those facts has been provided to the Complainant’s representative by the Commission on multiple occasions.

2.39 It is factually not the case that the Commission endorsed or approved of the Terms of Service and Privacy Policy of WhatsApp that were in place at the time of the Complaint, or indeed of any other organisation. Moreover, irrespective of any feedback that may or may not have been provided to Facebook, WhatsApp, or any other organisation, the Commission always emphasises that the consultation function is entirely distinct from any statutory inquiries, investigations, or decisions of the Commission. I also emphasise that this decision-making process was also functionally independent of the procedure conducted by the Investigator that led to the Final Inquiry Report, just as the statutory inquiries are functionally independent from any and all consultations with the Commission. The factual premise of the allegation is incorrect, and the test for bias has not been met. WhatsApp has made no particular submission, in this regard.

TRANSLATION ISSUES

2.40 Having been furnished with the Preliminary Draft, the Complainant’s representative wrote to the Commission by way of email dated 28 December 2021. It argued in that email that:

“... our complaint was filed with the [German Federal DPA] and the [German Federal DPA] has so far clearly insisted, that all communication must take place via the [German Federal DPA] and in German. This is a clear legal requirement under the GDPR and the German VwVfG, that the [German Federal DPA] and [the Complainant’s representative] are bound

¹³⁰ Open letter of Complainant’s representative, page 3, [https://noyb.eu/sites/default/files/202005/Open%20Letter noyb GDPR.pdf](https://noyb.eu/sites/default/files/202005/Open%20Letter%20noyb%20GDPR.pdf).

¹³¹ *ibid.*

to observe, as previously confirmed by the [Commission]. We are surprised that the latest communication was (again) not observing these clear procedural requirements.”

2.41 The Commission by way of response dated 30 December 2021 clarified that “... [i]n circumstances where Irish procedural law is applicable to this inquiry process, the [Commission] will not be providing a German language translation of the Preliminary Draft Decision.” The Complainant’s representative responded by email dated 30 December 2021 alleging, *inter alia*, that the Commission “... has repeatedly and strategically withheld documents from us” and that in its view not providing a Germanlanguage copy of the Preliminary Draft would be contrary to law. The Commission responded on 31 December 2021 stating that the Commission’s position had already been outlined, and that “... any of your queries regarding the [German Federal DPA] position ought to be directed to [German Federal DPA].”

2.42 The Complainant’s representative wrote to the Commission once again by way of email dated 7 January 2022. It stated that:

“... we would like to inform you that we have received a response from the [German Federal DPA] today, confirming that the relevant documents will be translated to German. We will await this translation in accordance with German law and properly file our response with the [German Federal DPA] in German, to ensure full compliance with the applicable German procedural laws. We will apply the four week deadline from the time we received the documents in German, similar to the deadline set by the [Commission] once the English documents were provided.”

2.43 The Complainant’s representative went on to seek confirmation that the existing deadline for receipt of submissions was therefore obsolete. The Commission responded by letter dated 17 January 2022, in which a lengthy explanation was provided as to why the Commission considered the Complainant’s representative’s position to be incorrect as a matter of law, and furthermore obstructive. The Commission nonetheless agreed to extend the deadline for the provision of submissions by a further four weeks.

2.44 Separately, the Commission received correspondence from the German Federal DPA, which clarified its position on the question of German law raised by the Complainant’s representative, in this regard. The email, dated 25 January 2022, stated that in its view:

“... it is exceptionally not necessary to provide a translated version in advance. We already provided the translated draft report to [the Complainant’s representative] in August 2020. We believe the facts haven’t changed substantially. We referred to the binding decision in [July] 2021 from which at least a short statement is available in German...[w]e have informed [the Complainant’s representative] of this view.”

2.45 On this basis, the Commission wrote to the Complainant's representative's legal advisors by letter dated 27 January 2022 clarifying the position of the German Federal DPA, and stating that the extended deadline stood. The Complainant's representative's legal advisors replied by letter also dated 27 January 2022, seeking copies of correspondence between the German Federal DPA and the Commission in this regard. The Commission responded by letter dated 27 January 2022 seeking copies of correspondence the Complainant's representative's legal advisors had received from the German Federal DPA, and stating that if a difference of opinion did exist between the Commission and the German Federal DPA, the appropriate channel for the resolution of such a difference of opinion was the cooperation and consistency mechanisms provided for by the GDPR.

2.46 The Complainant's representative's legal advisors wrote to the Commission once again by letter dated 1 February 2022. It was set out in that letter that the Complainant's representative was informed directly that

"... the [German Federal DPA] takes the view that under German law a Submission on a Preliminary Draft Decision is not necessary as Submissions under German law are only necessary on factual elements. Our client's understanding, therefore, is that the position of the [German Federal DPA] is not that a translation is not required, but in fact that Submissions are not required under German law. However if such Submissions are necessary, it would have to be translated. This seems to be at odds with the view of the [Commission] that the Submissions are necessary, but the translation is not."

2.47 The Complainant's representative's legal advisors wrote to the Commission by letter dated 3 February 2022 seeking confirmation that the position as outlined in the letter dated 1 February 2022 was correct. The Commission replied by letter dated 3 February 2022 confirming that while the Complainant's representative was invited to make submissions, at no point did the Commission assert that such submissions were necessary. The Commission also clarified that the German Federal DPA, as had already been outlined by the Commission, did not view it necessary to translate the Preliminary Draft into German.

2.48 No further correspondence on the question of translation took place. I am satisfied based on the position confirmed by the German Federal DPA and the Commission's own legal position in this regard, that the question of translation in this Inquiry has been dealt with in accordance with law.

ALLEGATION THAT COMPLETE DOCUMENTS HAVE NOT BEEN FURNISHED TO THE COMPLAINANT'S REPRESENTATIVE

2.49 In the Complainant's representative's email dated 28 December 2021, a further argument was made in relation the furnishing of relevant documents it by the Commission. In the email, the Complainant's representative stated:

“In addition, it seems the [Commission] is (again) not providing us with the relevant files, submissions and other documents in this case. We therefore kindly ask you to provide these documents by 31.12.2021 via the [German Federal DPA]. We are not in a position to make submissions on the “Preliminary Draft Decision” without having full access to the files of the case.”

2.50 The Commission’s response dated 30 December 2021 confirmed that “[the Complainant’s representative] *has received all relevant materials*”. The Complainant’s representative sought by further correspondence dated 30 December 2021, “... a confirmation under oath, that the [Commission] *has not only provided us with what it deems “relevant” documents, but all communication between WhatsApp Limited or any affiliated entity (including its parent company, legal representatives and alike) that relates to this complaints procedure.*” The Commission clarified by response dated 31 December 2021 that the Commission “...*has provided [the Complainant’s representative] with all relevant material, but, as previously outlined, this does not extend to appending every item of minor procedural correspondence exchanged between the parties*”.

2.51 Separately, the Complainant’s representative’s legal advisors wrote to the Commission on 5 January 2022, in relation to a separate, own-volition inquiry into WhatsApp that the Commission has concluded. The decision in that inquiry is currently subject to a judicial review and a statutory appeal before the Irish courts. Its legal advisors argued that “... *while it appears the substance of our client’s Complaint was considered in the Own Volition Inquiry, we have a serious concern that our client’s right to fair procedures has been breached, perhaps irreparably.*” The Complainant’s representative’s legal advisors went on to seek sight of the pleadings in the judicial review and statutory appeal on this basis and in order to enable the Complainant’s representative to decide if it wishes to apply to be joined as a party to the said proceedings.

2.52 The Commission responded to this correspondence by two letters dated 17 January 2022. In the first letter, it set out that:

“Your client is in receipt of the submissions made by WhatsApp in relation to the substantive issues under examination in the WhatsApp Inquiry, being two sets of submissions filed on 11 March 2019 and a further submission (in respect of the Draft Inquiry Report), made on 22 June 2020.

It is unclear why your client persists in contending otherwise.

If your client thinks it has seen reference, within the body of the [Preliminary Draft], to material it believes was submitted to the inquiry by WhatsApp, but which your client has not yet seen, please advise. On notification of such reference(s), we will deal with the matter forthwith.”

2.53 In the second letter of the same date, and specifically in relation to the question of sight of pleadings in the unrelated appeal and judicial review, the Commission explained that:

“The Commission’s findings in Inquiry IN-18-12-2 likewise relate to a broad range of issues, including, inter alia, the specific issue referenced in your letter dated 5 January 2022, i.e. whether WhatsApp’s processing of personal data on the basis of Article 6(1)(b) of the GDPR satisfy the GDPR’s transparency requirements.

The mere fact that there may be an overlap between an issue addressed in Own-Volition Inquiry IN-18-12-2, and an issue raised by a complainant represented by your client in a separate inquiry, does not give your client any right to be heard in relation to Own-Volition Inquiry IN-18-12-2. Third parties, such as your client, do not have any right to be informed of, or heard in respect of, an own volition inquiry.

In the circumstances, there has been no failure to observe your client’s right to be heard.”

2.54 For the reasons articulated in the above extracts from correspondence from the Commission to the Complainant’s representative and/or its legal advisors in relation to the provision of relevant documents in general, and in relation to the provision of pleadings in the proceedings in question, I am satisfied that all relevant documents have been provided to the Complainant’s representative and no question of a breach of fair procedures arises. In particular, I note that aside from the reference to the said pleadings, the Complainant’s representative has not referred to any specific documents which it believes to exist and of which it would like sight.

2.55 I am therefore satisfied that fair procedures have been followed in this and every regard thus far throughout the Inquiry.

3. THE SCOPE OF THE COMPLAINT AND INQUIRY

PROCEDURAL ISSUES SURROUNDING THE SCOPE OF THE COMPLAINT

3.1. The Complainant’s representative also alleged that in determining the scope of the Complaint and in not allowing it to revise the scope of that Complaint, the Commission was acting contrary to the Complainant’s right to fair procedures, with a specific focus on German procedural law (which has been dealt with above).

3.2. The Complainant’s representative wrote to the Investigator by letter dated 19 April 2019, and addressed the issue of the scope of the Complaint further. The Complainant’s representative stated that *“we reserve the right to amend our arguments should one of the controllers seek to depart from the factual or legal premises our complaints were based on.”* It was also emphasised, in that regard, that *“the complaints explicitly states that the complaints are based on our knowledge at the time of*

submission". Contrastingly, WhatsApp argued that the Complaint's scope should be strictly limited to processing that was processed on foot of consent.¹³²

3.3. In the Draft Inquiry Report, the Investigator relied on a statement in the Complaint which read:

*"For practical reasons, the scope of this complaint is explicitly limited to any processing operations that are wholly or partly based on Article 6(1)(a) and/or Article 9(2)(a) of the GDPR. Our current understanding is, that these are used as bases for all processing operations described in the controller's privacy policy..."*¹³³

3.4. Having outlined the scope, the Complaint then states that "... [n]evertheless, nothing in this complaint shall indicate that other legal bases the controller may rely on are not equally invalid or may not be equally the subject of subsequent legal actions."²³⁷ This qualifying remark, while alluding to the fact that the Complainant may have other views in relation to other legal bases for data processing carried out by WhatsApp, is evidently not one that describes the character of the Complaint in question. While such a remark clearly refers to hypothetical positions the Complainant may have or take in the future, it cannot alter the limiting character of the preceding statement in and of itself. It instead clarifies that the Complainant's representative reserves its position in respect of any other legal bases on which WhatsApp may or may not rely.

3.5. Having taken an objective reading of the Complaint, the Investigator concluded that the issues that arose were:

- **Issue (a):** the acceptance of the Terms of Service and/or Data Policy was an act of consent;
- **Issue (b):** WhatsApp cannot lawfully rely on necessity for the performance of a contract to process data arising out of the data subject's acceptance of those same documents;
- **Issue (c):** WhatsApp misrepresented the legal basis for processing this data; and
- **Issue (d):** WhatsApp failed to provide the necessary information regarding its legal basis for processing this data.

3.6. The Investigator went on to consider the Complainant's representative's submissions that the Complaint constituted an *"introductory request"*,¹³⁴ and that the scope should be expanded to include, *inter alia*: "... an all-encompassing assessment of the legal basis for every type of processing performed by WhatsApp in respect of the data subject"; "... an assessment of which aspects of the WhatsApp Terms of Service are relevant contractual terms for the purposes of processing under Article 6(1)(b) GDPR. The complainant submits that assessment should

¹³² WhatsApp submissions on Preliminary Draft, *inter alia*, paragraphs 2.6, 4.3, 7.4, 7.9(A), 8.1.

¹³³ Complaint, paragraph 1.6.

²³⁷ Complaint, Paragraph 1.6.

¹³⁴ Complainant's representative's submissions on Draft Inquiry Report, paragraph 2.3.

*involve a direct assessment of German contract law by the [the Commission].”; ... an exhaustive determination of which parts of the Terms of Service are "binding" on the data subject (as opposed to "declaratory" contractual language, which the complainant submits is not binding on the data subject)".*¹³⁵ WhatsApp by contrast argued that the scope should be confined to the contents of the Complaint.¹³⁶

3.7. The Investigator gave consideration to these submissions and ultimately did not revise his view.¹³⁷ WhatsApp’s view was that, contrary to both the view of the Investigator and the Complainant’s representative, the Complaint should be strictly limited to data processing carried out, as a matter of fact, on the basis of consent.¹³⁸ The Investigator found that it was not necessary to engage in a factual “*trawl*” of each one of WhatsApp’s processing operations, but instead to carry out a legal and factual analysis based on the objective content of the Complaint itself.¹³⁹ This was not based on an assessment of the “will” of the Complainant, hypothetical or otherwise, but simply on an assessment of the content of the Complaint.

3.8. At this point, I will make an assessment as to whether the Complainant’s representative’s specific allegations of procedural unfairness in how this was addressed by the Commission thus far have merit. In the “open letter” to which I have already referred, the Complainant’s representative alleged that “... *the Investigator departed from the applications that were made in accordance with [German] procedural law and decided to investigate only certain elements of our complaint and to reinterpret our requests.*”¹⁴⁰

3.9. It does not seem to me that the above quotation is an accurate characterisation of what has taken place. I have already (as had the Investigator) set out views on why German procedural law does not apply to the activities of the Commission. The merits or otherwise of the Investigator’s objective analysis of the content of the Complaint is addressed later in this section. I do not accept, however, that there is, in principle, a procedural defect in limiting the scope of a complaint-based inquiry to the objective contents of the very Complaint that led the Commission to conduct an Inquiry. As well as conforming to Section 113 of the 2018 Act (set out earlier in this Section of the Schedule), this approach is perfectly logical.

3.10. The Complainant’s representative’s arguments in relation to any alleged procedural defects in the manner in which the scope of the Complaint is to be determined, i.e. by the objective content of the Complaint, are based on German administrative law, and particularly on the VwVfG. Insofar as that those arguments are based on German law, for reasons already

¹³⁵ Final Inquiry Report, pages 11-13.

¹³⁶ WhatsApp’s submissions on Draft Inquiry Report, paragraph 2.12.

¹³⁷ Final Inquiry Report, pages 13-22.

¹³⁸ WhatsApp submissions on Draft Inquiry Report, paragraph 1.3(D).

¹³⁹ Final Inquiry Report, paragraph 62.

¹⁴⁰ Open letter, page 6 https://noyb.eu/sites/default/files/2020-05/Open%20Letter_noyb_GDPR.pdf.

set out, the Commission cannot consider those arguments, save to the extent that they raise issues of either Irish or EU law.

- 3.11. Moreover, as I have set out, the decision to conduct a complaint-based Inquiry arising out of the contents of a Complaint seems to me to be a perfectly logical approach. The alternative would be an open-ended procedure, where the content of a “complaint” would crystallise at some unspecified future date. The inherent problem with such an approach is that it would not amount to an inquiry based on the Complaint which was lodged with the Commission, but would instead be an inquiry directed by the Complainant (or their representative), with its subject matter and steps dictated on an evolving and ongoing basis. Furthermore, it is unclear how it could be said that such an approach constitutes a complaint that concerns personal data relating to the Complainant. This would presumably only occur once a complainant is satisfied of receipt of all information they might require, and has been afforded the opportunity to amend the complaint itself based on the submissions of the other party.
- 3.12. The unfairness that could arise from such an approach stems from the fact that it would, in effect, enable a form of *post-hoc* amendment to an existing complaint over the course of an indefinite period of time, which could only come to an end at a time and in a manner of a complainant’s choosing. This would not only amount to a fundamentally one-sided approach, but would also alter the character of the inquiry to the extent that it could no longer be described as “complaint-based”, but rather “complainant-led”. Such a request following a complaint, to the effect that the Commission would consider a series of extremely broad requests to fundamentally alter an inquiry and deviate from the initial complaint it had begun to investigate, is therefore procedurally problematic. The Complainant’s representative has pointed to no legal provision that mandates this, aside from assertions made in relation to German law that have already been addressed herein.
- 3.13. This also applies to aspects of the Complaint that either reserve the Complainant’s position or express views on hypothetical investigative and/or corrective powers that, in the Complainant’s and/or the Complainant’s representative’s view, the Commission should exercise. I see no breach of fair procedures in considering the Complaint as a whole in order to determine the exact infringements being alleged. There is no particular procedural right to make generalised requests to the Commission to either conduct broad-based investigations or exercise particular corrective powers in the context of a complaint.
- 3.14. The Complainant’s representative having lodged the Complaint via the Hamburg SA, responded to the Draft Inquiry Report, which set out clearly the submissions of WhatsApp and the Investigator’s views on same. The Complainant’s representative has also been afforded the opportunity to make submissions on a draft of this Decision. No suggestion has been made that the alternative procedure proposed by the Complainant’s representative is a requirement of Irish law, nor that the procedure that has been followed in relation to the scope breaches any rules of fair procedures in Irish law. Moreover, I am unaware of any case

law or statutory provisions in Irish law or EU law that suggests that such an approach is contrary to the Complainant's right to fair procedures, and the Complainant's representative has not referred to any such law in its submissions.

SUBSTANTIVE SCOPE OF THE COMPLAINT

3.15. Put in high-level terms, this complaint-based Inquiry concerns the requirement under EU data protection law for any entity collecting and processing personal data to establish "a lawful basis" for the processing under Articles 6 GDPR. This particular Complaint was lodged by reference to WhatsApp and its lawful basis for processing user personal data and "special category" personal data. I have set out, in summary form, the contents of the Complaint and arguments contained in it at Section 2 of this document.

3.16. "Personal data" is defined under Article 4(1) GDPR as:

"... 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".

3.17. Moreover, Article 4(13) GDPR defines the "genetic data" referred to above as:

"... personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question".

3.18. Article 4(14) GDPR defines "biometric data" as:

"... personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

3.19. Finally, "data concerning health" is defined by Article 4(15) GDPR as:

"... personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

3.20. The other special categories or personal data referred to in Article 9 GDPR are not defined in the GDPR.

3.21. As set out above, Article 6 GDPR sets out the lawful bases for the processing of personal data. The provisions of Article 6 that arise in this complaint-based Inquiry are the first two lawful basis listed in the Article, in Articles 6(1)(a) and 6(1)(b) GDPR. Article 6(1) GDPR states:

“6. 1 Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”

3.22. A number of conditions for consent are enumerated in Article 7 GDPR:

“1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”*

3.23. Article 13(c) GDPR requires data controllers to provide information to data subjects on *“the purposes of the processing for which the personal data are intended as well as the legal basis for the processing”*.

3.24. Article 12(1) GDPR requires that *“[t]he controller shall take appropriate measures to provide any information referred to in Articles 13 and 14...to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language...”*.

3.25. Unusual circumstances arise in relation to this Complaint because of its very starting-point, namely, the assertion that accepting WhatsApp’s Terms of Service (and, allegedly, Privacy Policy) purported to bring all personal data processing under the lawful basis of consent for the purposes of Article 6(1)(a) GDPR. This starting point was rejected in WhatsApp’s submissions. While the Investigator did not agree with the entirety of WhatsApp’s submissions by any means, he also rejected this premise. For the reasons set out below, I also rejected it in the Draft Decision. This rejection of the foundational premise of the Complaint has inevitably rendered the overall subject-matter of the Complaint effectively less cohesive.

3.26. The Complaint also refers to processing of special category data covered by Article 9 GDPR. The Complainant’s representative’s submissions on the Draft Inquiry Report make further arguments, in this regard, particularly in relation to WhatsApp’s alleged ability to infer religious views, sexual orientation, political views and health status. No evidence is presented for this speculative assertion based on who the Complainant interacts with.¹⁴¹

3.27. My view, as expressed in the Draft Decision, was that, for the reasons set out above and the additional reasons set out below where I had made conclusions on the scope of the Complaint in the Draft Decision, the Complaint even taken at its height quite clearly only concerns data processing arising out of the act of acceptance. The Complainant’s representative’s central arguments on “forced consent” are predicated on the assertion that the acceptance is forcing a consent to personal data processing for the purposes of the GDPR.

¹⁴¹ Complaint, paragraph 1.3.; Complainant’s representative’s submissions on Final Inquiry Report, paragraph 5.2.1.

- 3.28. On this basis, I did not accept, in the Draft Decision and the schedule to the Draft Decision, that the processing of sensitive categories of personal data on the basis of Article 9 GDPR consent fell within the scope of this Inquiry. In the Draft Decision and the schedule to the Draft Decision, I noted that there was no evidence that WhatsApp processes special category data at all. I further noted, in the Draft Decision and the schedule to the Draft Decision, in relation to the Complainant’s representative’s speculative assertion relating to WhatsApp’s ability to infer such data, that messages between users are end-to-end encrypted. WhatsApp agrees with this position.¹⁴²
- 3.29. WhatsApp takes a narrower view on the scope of the Complaint as determined by the Investigator and as determined by the Commission in the Preliminary Draft. In particular, WhatsApp is of the view that the scope of the Complaint relates solely to the allegation of “forced” consent, and that the only issue that falls to be addressed is the allegation that the Complainant was forced to consent to the Terms of Service and Privacy Policy (consent here having the meaning it has in Article 6(1)(a) GDPR).¹⁴³
- 3.30. In making this argument, WhatsApp relies on the EDPB’s Guidelines 09/2020 on relevant and reasoned objections under Regulation 2016/679 (“the **RRO Guidelines**”). The RRO Guidelines state that in:
- “... procedures based on a complaint or an infringement reported by a [concerned supervisory authority], the scope of the procedure (i.e. those aspects of data processing which are potentially the subject of a violation) should be defined by the content of the complaint or of the report shared by the [concerned supervisory authority]: in other words, it should be defined by the aspects addressed by the complaint or report.”¹⁴⁴*
- 3.31. While I noted, in the Draft Decision, that the RRO Guidelines self-evidently concern relevant and reasoned objections made during the Article 60 Process and not the conduct of cross-border inquiries at Member State level prior to the Article 60 Process, as is the case here, guidelines of the EDPB are nonetheless significant but non-binding documents as regards the work of the Commission. In the Draft Decision, I was satisfied that applying the principle articulated paragraph above, the Complaint still raises issues relating to the obligation to rely on consent and therefore, by implication, WhatsApp’s inability to rely on another legal basis. In circumstances where WhatsApp is seeking to rely on necessity for the performance of a contract, that legal basis is the one that stands to be considered at the level of principle.

¹⁴² WhatsApp submissions on Preliminary Draft, paragraph 7.9(A).

¹⁴³ WhatsApp submissions on Preliminary Draft, paragraph 1.3(A).

¹⁴⁴ RRO Guidelines paragraph 27, as cited in WhatsApp submissions on Preliminary Draft, paragraph 4.3.

- 3.32. WhatsApp emphasises that the Complainant’s representative’s arguments in relation to its entitlement to rely on 6(1)(b) GDPR were made not in the Complaint itself, but in submissions. The reality is that the Complaint was made on an apparently erroneous assumption (that seems to be now accepted by all parties), i.e. that WhatsApp was relying on consent for some of the processing in question. The Complainant’s representative is nonetheless persisting in the position it states it has always held, i.e. (1) that WhatsApp is obliged to rely on consent because no other lawful basis is applicable, and (2) that the conditions for consent have not been met, therefore the processing is unlawful. I expressed the view, in the Draft Decision and schedule to the Draft Decision, that in circumstances where WhatsApp is relying on a lawful basis other than consent, the Complainant’s representative position that it is not entitled to do so and must rely on consent (for which the Complainant’s representative says it has failed to meet the requisite conditions) falls clearly within the scope of this Complaint.
- 3.33. On the question of scope, WhatsApp also disputes the inclusion of matters of transparency.¹⁴⁵ In my view, it has been established in the analysis of the Investigator, the analysis in the Preliminary Draft, and herein, as well as in the Complaint itself, that matters of transparency clearly arise. The Complaint specifically asserting that it is difficult to determine the relationship between particular lawful bases relied on by WhatsApp and individual categories of data, as set out above. Moreover, the Complaint clearly raises issues about how the “engagement flow” and act of acceptance were presented to the Complainant. These aspects of the Complaint, for these reasons and reasons already set out, clearly relate to the transparency provisions of the GDPR.
- 3.34. In the Draft Decision, I found that the Complaint is therefore one about whether the Terms of Service (which is the contract with the user) are a deliberately veiled and inadequate means of forcing consent under GDPR, or whether they are, as WhatsApp contends, a contract with the user for which certain data processing is necessary in order to perform that contract.
- 3.35. Having reviewed and considered all of the material submitted by the Complainant’s representative, I concluded, in the Draft Decision, that the core of the issues raised by the Complainant were as follows:
- a. Accepting the Terms of Service offered by WhatsApp in April 2018 specifically constituted an act of consent to personal data processing under the GDPR. The precise extent of the processing complained of is unclear in the Complaint. A particular focus is, however, placed on both processing in order to deliver behavioural advertising, and on special category data. The Complainant takes issue with any unlawful processing based on this agreement, whatever that agreement’s legal character might be.

¹⁴⁵ WhatsApp submissions on Preliminary Draft, paragraph 2.6 and 8.1.

- b. The Complainant argues that 6(1)(a) GDPR, i.e. consent, is the mandatory, default lawful basis for personal data processing where there is a contract or agreement primarily concerned with personal data processing, or where the “declaration of intent” of the parties primarily concerns data processing.
 - c. Consent under the GDPR is simply an indication of agreement by the data subject according to the Complainant. The necessary attributes of freely given, specific, informed and unambiguous are merely “conditions for its validity”, but not features of objective “consent”.
 - d. As an alternative to point (a), WhatsApp is not entitled to rely on the “necessary for the performance of a contract” legal basis under Article 6(1)(b) GDPR other than for very limited processing. It therefore cannot rely on this as an alternative legal basis to consent for the acceptance of the Terms of Service as a whole. In this regard, the Complainant argues that the “purpose” of the contract (here, to deliver a social media service) must be considered.
 - e. On the basis of all of the above, the Complainant contends that clicking accept was an attempt by WhatsApp to seek consent under the GDPR - just not **valid** consent. The Complainant describes this as “forced consent”, in that the only choice a user had in April 2018 was to stop using the service, and “hidden consent”, in that some of the description of the WhatsApp service in the Terms of Service implicitly relies on processing of personal data.
 - f. The Complainant contends that WhatsApp leads data subjects to believe that it relies on consent as lawful basis for personal data processing and/or is not transparent about its lawful bases for processing personal data.
- 3.36. It is important to note, at this juncture that, as set out in paragraph 2.19 of this Decision, the EDPB, in the Article 65 Decision, took a different view on the scoping of the Complaint.
- 3.37. WhatsApp’s position is that the Terms of Service forms a contract with its users for the use of its free service. The Commission observes that this is delivered in the form of a “Click Wrap” agreement that the user signs up to when clicking “Accept” on the Terms of Service and it looks similar to an industry standard format for such agreements. Its intention was, WhatsApp says, to rely on the legal basis of Article 6(1)(b) GDPR (necessary for the performance of a contract) for processing carried out on foot of the acceptance of the Terms of Service (and, for other separate processing, it would rely on other legal bases).
- 3.38. In this regard, it claims that the processing is necessary for the performance of the contract with the user and that the Privacy Policy further sets out, in more detail, the other

- legal bases that would be relied on for other processing operations. WhatsApp rejects the idea that it sought to persuade users that consent was the legal basis for all personal data processing. It further accordingly rejected the Investigator's analysis of whether valid consent was collected at the point of acceptance of the Terms of Service, on the basis that WhatsApp never sought to rely on consent.
- 3.39. The Investigator analysed each of the arguments made in the original Complaint submitted. This was, in my view, a sensible and correct approach. This was not an "own volition" Inquiry where the Commission was entitled to scope matters of risk which it decided warranted investigation. While it is normally the role of the Investigator to focus on the establishment of facts, to set out what elements of the GDPR are engaged against those facts, to come to a view on whether there are likely infringements identified which will then be the subject of further legal analysis and ultimately decision-making by the Commission, this case is somewhat different.
- 3.40. The facts to be established are fairly limited and are largely relating to the wording of WhatsApp's Terms of Service and its Privacy Policy, and the design of its "User Engagement Flow" introduced in April 2018 to guide users through the process of acceptance process. In fact, it appears to me that the Investigator ended up devoting time responding to legal and theoretical assertions of the Complainant's representative, such as the argument that consent is a *lex specialis* and therefore the mandatory legal basis where a contract primarily concerns personal data processing. Consequently, the Final Inquiry Report contains more legal analysis and argument than might otherwise have been the case (relative to a draft decision). I have considered all of the analysis of the Investigator carefully and, in some instances, I adopt it and concur with it. In other instances I reject it, replace it, and explain why.
- 3.41. Another feature of the Complaint is a section entitled "*Applications*". In this section, the Complainant requests an investigation of a very specific nature, and sets out the corrective powers that the Complainant believes should be imposed i.e. an administrative fine and a prohibition on the "relevant processing operations". This section asks the Commission to:

"... fully investigates this complaint, by especially using its powers under Article 58(1)(a), (e) and (f) of the GDPR, to particularly determine the following facts:

- (i.) which processing operations the controller engages in, in relation to the personal data of the data subject,*
- (ii.) for which purpose they are performed,*
- (iii.) on which legal basis for each specific processing operation the controller relies on and*
- (iv.) he/she additionally requests that a copy of any records of processing activities (Article 30 of the GDPR) are acquired."*

- 3.42. The right to lodge a complaint with a supervisory authority is governed by Article 77 GDPR. Article 77(1) states how a complaint may be made: “... *every data subject shall have the right to lodge a complaint with a supervisory authority...if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*” [emphasis added]. Neither the request above, nor a request to impose specified corrective powers, can be considered to constitute part of a complaint made in accordance with Article 77(1) GDPR. The Complaint does not specify any processing operations or any alleged infringements of the GDPR in the above request, but simply asks the Commission to gather information on its behalf. Neither the GDPR nor the 2018 Act confer a complainant with a particular right to make such a request, nor to specify what corrective powers should be imposed in circumstances where the supervisory authority is of the view that an infringement has occurred/is occurring. To the extent that such an approach might be known to German law, I have already set out in detail why I do not accept that such law is applicable to the exercise of my functions.
- 3.43. In those circumstances, it was for the Investigator, and ultimately for me as decision-maker, to carry out an objective reading of the Complaint. In so doing, I must consider not only the content of the Complaint, but also the legal framework by which the Commission is bound. It is also necessary that an inquiry conducted on foot of a complaint must be feasible and workable. According to Article 77(1) GDPR, a complaint should relate to data processing that, in a complainant’s view, infringes the GDPR. There is a lack of reasonable specificity in the above request in relation to processing operations or alleged infringements.
- 3.44. Any request to investigate all processing, or hypothetical processing, particularly a request of such an indefinite nature, does not, in my view, conform to the requirements of Article 77 GDPR. Such a request does not specify any data processing or any alleged infringement, and would result in a practically unworkable inquiry. Rather than being a complaint about specific processing operations, the Complaint in this matter has, at times, strayed into the territory of instructing the Commission to conduct an open-ended inquiry, and to direct that inquiry and the Commission’s resources in a manner determined by the Complainant and/or the Complainant’s representative. It is instead for the Commission to decide on the manner in which a reasonably specific Complaint is to be investigated.
- 3.45. The Decision therefore reflects the outcome of my determination on the matters relating to the procedural and scope issues. It is important to again note that, as set out in paragraph 2.19 of this Decision, the EDPB, in the Article 65 Decision, took a different view on the scope of the Complaint. In the circumstances, the views expressed in this Schedule 1 must be read in conjunction with the corresponding assessment and determination of the scope of the Complaint made by the EDPB in the Article 65 Decision, as set out in Schedule 2 to this Decision.

SCHEDULE 2