NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

In the matter of the General Data Protection Regulation

DPC Case Reference: IN-18-5-5

In the matter of LB (through NOYB) v Facebook Ireland Limited

Draft Decision for the purposes of Article 60 GDPR of the Data Protection Commission made pursuant to Section 113(2)(a) of the Data Protection Act 2018

Further to a complaint-based inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DRAFT DECISION

Decision-Maker for the Commission:

[DRAFT – BEARS NO SIGNATURE]

Helen Dixon
Commissioner for Data Protection

Dated the 6th October 2021

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

Contents

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

1. INTRODUCTION AND PROCEDURAL BACKGROUND

PURPOSE OF THIS DOCUMENT

1.1 This document is a draft Decision ("the **Draft Decision**") of the Data Protection Commission ("the **Commission**") in accordance with Section 113(2)(a) 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 Facebook Ireland Limited ("**Facebook**") 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 Ms. L.B. ("the **Complainant**"). The complaint was referred to the Commission by the Austrian Data Protection Authority, *Die Österreichische Datenschutzbehörde* ("The **Austrian DPA**") on 30 May 2018 ("the **Complaint**"). In advance of the preparation of this Draft Decision, a preliminary draft of this document ("the **Preliminary Draft Decision**") was circulated to Facebook and the Complainant's representative so as to enable them to make submissions on my provisional findings. The submissions of these parties have been taken into account in finalising this Draft Decision.

1.3 Further details of procedural matters and a chronology pertaining to the Inquiry are set out in the Schedule to this decision.

2. FACTUAL BACKGROUND AND THE COMPLAINT

FACTUAL BACKGROUND

2.1 Facebook is an online social network and social media platform. In order to access the Facebook platform, a prospective user must create a Facebook account. To create a Facebook account, a prospective user is required to accept a series of terms and conditions, referred to by Facebook as their Terms 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 Facebook. It is only on acceptance of the Terms of Service that the individual becomes a registered Facebook user.

2.2 In April 2018, Facebook 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. Among the obligations under the GDPR, as under Directive 95/46/EC, was the fundamental requirement that data controllers have a lawful basis for any processing of personal data they undertake. Legal bases provided for in the GDPR include consent of the data subject, necessity for the purposes of the performance of a contract with the data subject or processing necessary for the purposes of the legitimate interests of the data controller. In addition, under the GDPR, controllers 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 (of personal data) and there must be transparency in the communication of such information to individual users. Prior to the GDPR taking legal effect, no detailed requirement existed for a controller to explicitly state what legal basis they relied on in processing particular categories of personal data.

2.3 To continue to access the Facebook platform, 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 Facebook users by way of a series of information notices and options on the Facebook platform, referred to as an "engagement flow" or "user flow". The engagement flow was designed to guide users through the processing of deciding whether to accept the updated Terms of Service. The option to accept the updated "terms" was presented to users at the final stage of the engagement flow. The final stage of the engagement flow also contained embedded hyperlinks to the full text of the Terms of Service, the Data Policy and the Cookies Policy. As referenced in the full text of the Terms of Service, the Data Policy provides information to users on Facebook's processing of personal data in respect of the Facebook platform.

2.4 Existing users who were not willing to accept the new terms were advised of the option to delete their Facebook account. Such users were informed that they could no longer use the Facebook platform without accepting the new terms. Prior to deletion of the account, the users were also informed of the option to download a copy of their personal data which had undergone processing by Facebook.

2.5 Users who did continue through the new "engagement flow" were given the opportunity to consent or not to consent to a number of specific data processing activities, including the use of facial recognition. Provision of consent for such processing was not presented as a prerequisite for continuing to use the service. In other words, these were choices the user could make above and beyond the decision to sign up to the service, and users are free to use the service without providing consent to this processing.

2.6 Figures 2.1 and 2.2, below, are screenshots 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 screenshots are in German; an English translation can be found below.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

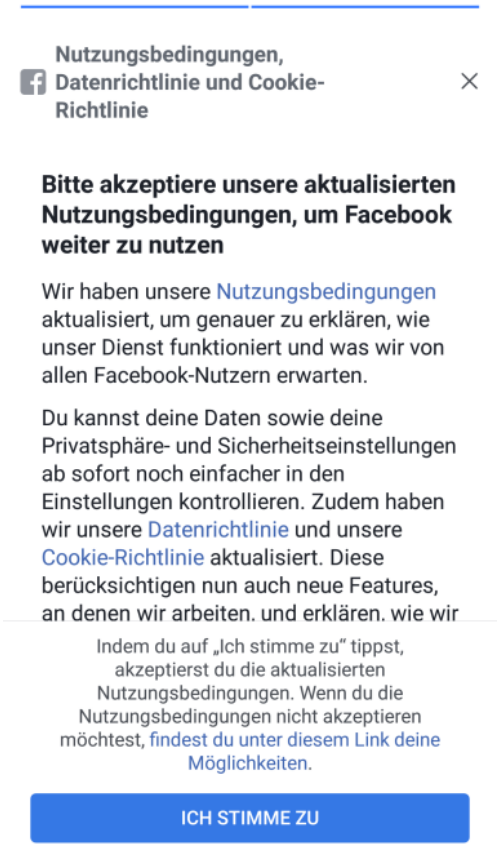

Figure 2.1

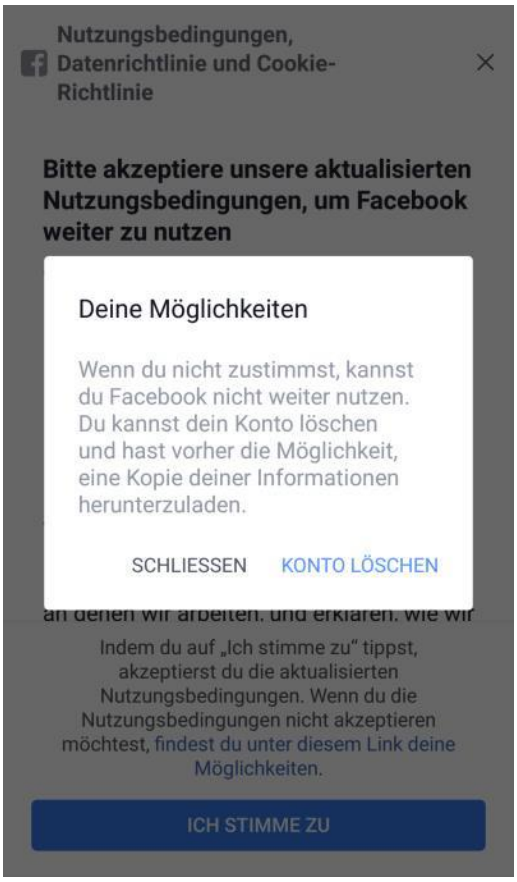

Figure: 2.2

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

Figure 2.1: "*Please accept our updated Terms of Service to continue using Facebook. We have updated our Terms of Service to explain in more detail how our service works and what we expect from all Facebook uses. You can now more easily control your data as well as your privacy and security settings in the settings. We have also updated our Data Policy and our Cookie Policy. These now also take into account new features that we are working on and explaining. By clicking "I agree", you accept the updated Terms of Service. If you do not want to accept the terms of use, you can find your options under this link.*"

Figure 2.2: "*If you do not agree, you can no longer use Facebook. You can delete your account and have the option to download a copy of your information beforehand. Close/Delete Account*".

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

2.8 The Complaint was made in the context of Facebook's updated Terms of Service and the requirement for existing users to accept the new terms to continue to access the Facebook platform.

2.9 In respect of the updated Terms of Service, the Complainant alleges that she was given a binary choice: either accept the Terms of Service and the associated Data Policy by selecting the "accept" button,[1] or delete her Facebook account. The Complainant's argument is predicated on the Data Policy being incorporated into the Terms of Service. This claim is disputed by Facebook.[2] The Complainant further alleges that Facebook 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*"[3] and did not give users a genuine choice to decline the updated terms without suffering detriment.

2.10 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*"[4] 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.*"[5] In connection with this, the Complainant expresses particular concern with reliance on Article 6(1)(b) GDPR as a legal basis for the processing operations detailed in the Terms of Services; extracts from the Terms of Services which relate to these processing operations are found below.

2.11 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.[6]

2.12 In the submissions on the Preliminary Draft Decision made on the Complainant's behalf, it is argued that the Commission has "*failed to investigate the relevant facts*".[7] As far as it has been possible to discern from the submissions, it appears that this assertion is linked to the Complainant's contention that the Commission has misconstrued the scope of the Complaint

[1] For completeness, it should be noted that Facebook disputes the claim that the Data Policy is part of the Terms of Service.
[2] Facebook Submissions on Draft Report, paragraph 7.1(A)
[3] Complaint, page 3.
[4] *Ibid.*
[5] 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.
[6] *Ibid*, page 6 and paragraph 2.3.4.
[7] Complainant Submissions on Preliminary Draft Decision, paragraph 4.1.

and/or failed to carry out particular acts or investigative steps that the Complainant has demanded of the Commission. I address this submission in the consideration of the scope of the Complaint below and in the Schedule to this Draft Decision. In reality, the essential facts relevant to this Complaint are simple and not in dispute; it is the legal assessment of these facts under the GDPR that requires determination in this Complaint.

2.13 The sections of the Terms of Service that relate to the data processing complained of are as follows:

> "*Our Services:*
>
> *Our mission is to give people the power to build community and bring the world closer together. To help advance this mission, we provide the Products and services described below to you:*
>
> *Provide a personalized experience for you:*
> *Your experience on Facebook is unlike anyone else's: from the posts, stories, events, ads, and other content you see in News Feed or our video platform to the Pages you follow and other features you might use, such as Trending, Marketplace, and search. We use the data we have - for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products - to personalize your experience.*
>
> *Connect you with people and organizations you care about:*
> *We help you find and connect with people, groups, businesses, organizations, and others that matter to you across the Facebook Products you use. We use the data we have to make suggestions for you and others - for example, groups to join, events to attend, Pages to follow or send a message to, shows to watch, and people you may want to become friends with. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.*
>
> *Empower you to express yourself and communicate about what matters to you:*
> *There are many ways to express yourself on Facebook and to communicate with friends, family, and others about what matters to you - for example, sharing status updates, photos, videos, and stories across the Facebook Products you use, sending messages to a friend or several people, creating events or groups, or adding content to your profile. We also have developed, and continue to explore, new ways for people to use*

technology, such as augmented reality and 360 video to create and share more expressive and engaging content on Facebook.

Help you discover content, products, and services that may interest you:
We show you ads, offers, and other sponsored content to help you discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Facebook Products. Our partners pay us to show their content to you, and we design our services so that the sponsored content you see is as relevant and useful to you as everything else you see on our Products.

Combat harmful conduct and protect and support our community:
People will only build community on Facebook if they feel safe. We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example, offering help, removing content, blocking access to certain features, disabling an account, or contacting law enforcement. We share data with other Facebook Companies when we detect misuse or harmful conduct by someone using one of our Products.

Use and develop advanced technologies to provide safe and functional services for everyone:
We use and develop advanced technologies - such as artificial intelligence, machine learning systems, and augmented reality - so that people can use our Products safely regardless of physical ability or geographic location. For example, technology like this helps people who have visual impairments understand what or who is in photos or videos shared on Facebook or Instagram. We also build sophisticated network and communication technology to help more people connect to the internet in areas with limited access. And we develop automated systems to improve our ability to detect and remove abusive and dangerous activity that may harm our community and the integrity of our Products.

Research ways to make our services better:
We engage in research and collaborate with others to improve our Products. One way we do this is by analyzing the data we have and understanding how people use our Products. You can learn more about

some of our research efforts.

Provide consistent and seamless experiences across the Facebook Company Products:

Our Products help you find and connect with people, groups, businesses, organizations, and others that are important to you. We design our systems so that your experience is consistent and seamless across the different Facebook Company Products that you use. For example, we use data about the people you engage with on Facebook to make it easier for you to connect with them on Instagram or Messenger, and we enable you to communicate with a business you follow on Facebook through Messenger.

Enable global access to our services:

To operate our global service, we need to store and distribute content and data in our data centers and systems around the world, including outside your country of residence. This infrastructure may be operated or controlled by Facebook, Inc., Facebook Ireland Limited, or its affiliates

.....

How do we use your information

We use the information we have (subject to choices you make) as described below and to provide and support the Facebook Products and related services described in the Facebook Terms and Instagram Terms. Here's how:

Provide, personalize and improve our Products.

We use the information we have to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads) and make suggestions for you (such as groups or events you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide where you have given your explicit consent); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products. Learn more about how we use information about you to personalize your Facebook and Instagram experience, including features, content and

recommendations in Facebook Products; you can also learn more about how we choose the ads that you see.

- *Information across Facebook Products and devices: We connect information about your activities on different Facebook Products and devices to provide a more tailored and consistent experience on all Facebook Products you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger. We can also make your experience more seamless, for example, by automatically filling in your registration information (such as your phone number) from one Facebook Product when you sign up for an account on a different Product.*

- *Location-related information: We use location-related information such as your current location, where you live, the places you like to go, and the businesses and people you're near-to provide, personalize and improve our Products, including ads, for you and others. Location related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Facebook Products (such as check-ins or events you attend).*

- *Product research and development: We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.*

- *Face recognition: If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create are data with special protections under EU law. Learn more about how we use face recognition technology, or control our use of this technology in Facebook Settings. If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.*

- *Ads and other sponsored content: We use the information we have about you-including information about your interests, actions and connections-to select and personalize ads, offers and other sponsored content that we show you. Learn more about how we select and personalize ads, and your choices over the data we use to select ads*

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

> *and other sponsored content for you in the Facebook Settings and Instagram Settings.*
>
> ***Provide measurement, analytics, and other business services.***
> *We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services. Learn how we share information with these partners.*
>
> ***Promote safety, integrity and security.***
> *We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to detect when someone needs help. To learn more, visit the Facebook Security Help Center and Instagram Security Tips.*
>
> ***Communicate with you.***
> *We use the information we have to send you marketing communications, communicate with you about our Products, and let you know about our policies and terms. We also use your information to respond to you when you contact us.*
>
> ***Research and innovate for social good.***
> *We use the information we have (including from research partners we collaborate with) to conduct and support research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. For example, we analyze information we have about migration patterns during crises to aid relief efforts. Learn more about our research programs."*

SCOPE OF THE COMPLAINT

2.14 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 in this regard (1) as between the parties and (2) as between the parties and the DPC in the course of establishing the substantive scope of the Complaint is included in the

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

Schedule. Also included in the Schedule are details of the approach I have adopted in determining the scope of the Complaint. In determining the precise parameters of the scope of the Complaint, I have had regard to the Complaint as a whole and, in particular, have taken note of the express statements in the Complaint which define its scope. I have also had regard to the Investigator's analysis in respect of the scope of the Complaint.

2.15 On his assessment of the Complaint, the Investigator concluded that there were four key issues to be analysed in the context of his Inquiry: [8]

a. Whether clicking "accept" on the Terms of Service was to be construed as an act of consent, or must be an act of consent, to the processing of personal data for the purposes of the GDPR – the Investigator's conclusions 1 and 2 of the Final Report address this issue

b. Whether Facebook could rely on Article 6(1)(b) GDPR as a lawful basis for processing personal data with respect to its Terms of Service – the Investigator's conclusion 3 of the Final Report addresses this issue

c. Whether Facebook misrepresented the legal basis for processing in a manner that caused the Complainant to believe that consent was relied upon – the Investigator's conclusions 4 and 10 of the Final Report address this issue

d. Whether Facebook had failed to provide the necessary information regarding its legal basis for processing in connection with its Terms of Service and Data Policy – the Investigator's conclusions 5, 6, 7, 8 and 9 of the Final Report address this issue

2.16 I agree 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 take a different view.

2.17 Issue (c), as identified by the Investigator, solely addresses the allegation that Facebook has misrepresented the lawful basis relied on in connection with the Terms of Service. I agree that this issue falls within the scope of the Complaint. Issue (d), however, was treated by the Investigator as a generalised assessment of whether Facebook's Data 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.*

[8] Final Report, paragraph 7.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

> *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."*[9]

2.18 It is on that basis that the Investigator interpreted the scope of the Complaint as comprising the allegation that the Data 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.*
>
> *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*."[10]

2.19 I do not accept that the factual question of whether Facebook "misled" the data subject (i.e. issue (c)) is a separate legal question from whether Facebook 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 Facebook has breached its transparency obligations, it logically follows that the Complainant will have been unlawfully "misled", whether deliberately or otherwise. If Facebook 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.

2.20 In the submissions on the Preliminary Draft Decision, the Complainant's representative argues that the questions answered by the Preliminary Draft Decision do "*not even come close*" to covering all aspects of the Complaint.[11] However, it is clear, as set out herein and in the Schedule, that this Complaint is limited to allegedly unlawful processing carried out on foot of the "agreement" i.e. the acceptance of the Terms of Service, and the extent to which the nature of that agreement was misleading. I therefore do not accept that the questions addressed in the Preliminary Draft Decision do not cover all aspects of the Complaint.

[9] Complaint, paragraph 1.3.
[10] *Ibid* page 3.
[11] Complainant Submissions on Preliminary Draft Decision, paragraph 4.2.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

2.21 The Complainant's submissions on the Preliminary Draft Decision further argue that there has been a failure to investigate the relevant facts. It is argued that there is a fundamental disagreement as to whether the agreement the Complainant has accepted is "a contract" or "a consent".[12] This issue was dealt with extensively in the Preliminary Draft Decision and is determined below in this Draft Decision.

2.22 While the Complainant's submissions on the Preliminary Draft Decision call for the Commission to engage in a thorough investigation as to the nature of this agreement, having regard to the scope of the Complaint, this is, in my view, entirely unnecessary 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 in relation to the fact that there is a contract between Facebook and the Complainant or the fact 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 Draft Decision and in the Schedule, is the lawfulness of the personal data processing and the transparency of the information provided.

2.23 On this basis, the issues that I will address in this Draft Decision are 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 Facebook 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.

3 ISSUE 1 – WHETHER CLICKING ON THE "ACCEPT" BUTTON CONSTITUTES OR MUST BE CONSENT FOR THE PURPOSES OF THE GDPR

WHETHER THE ACCEPTANCE IS CONSENT

3.1 As I have outlined in Section 2, the Complainant alleges that clicking on the "accept" button of the engagement flow presented to existing users in respect of Facebook's updated Terms of Service in April 2018 constituted an act of consent by the data subject for the purposes of Article 6(1)(a) GDPR. The first question to be considered is whether Facebook, via the updated Terms of Service, sought to obtain the Complainant's "consent" for the purposes of processing of personal data under those Terms of Service. Facebook's position, as noted above, is that it did not.

[12] *Ibid*, paragraph 4.3.1.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

3.2 In this regard, I note that the Complainant's position partly rests on several arguments to the effect that the design of the engagement flow is "*deceptive*".[13] The Complainant expresses particular concerns in respect of the final stage of the engagement flow and alleges that the acceptance process is set out in a misleading manner, such that a reasonable user would, and indeed the Complainant did in fact, believe that they are consenting for the purposes of Article 6 GDPR to data processing rather than simply signing up to a contract.[14] These arguments in relation to the alleged misleading nature of the user engagement flow will be considered as part of Issue 3 in the context of transparency requirements. This first issue is solely concerned with whether reliance is placed on the legal basis of consent.

3.3 In this context, I will first consider whether, as a matter of fact, Facebook sought to rely on consent at all as a legal basis. I will subsequently assess whether, as a matter of law, Facebook was obliged to seek consent as a legal basis for processing, as the Complainant argues.

3.4 In its submissions on the Draft Report made to the Investigator, the Complainant argues that the "*scope of application*" of consent and the "*conditions of validity*" under the GDPR must be distinguished. The Complainant further argues that the "*scope*" of consent is any "*expression of will by which the data subject indicates his consent to the processing of his personal data*".[15] The "*conditions of validity*" are, in the Complainant's view, the elements of the definition of consent set out in Article 4(11) GDPR. The Complainant further argues that "[t]*o come up with the crazy idea that a violation of the conditions of consent automatically leads to the inapplicability of these conditions is a legal shot in the foot.*"[16] The Complainant's position is that there are some circumstances in which only consent - and no other legal basis - is applicable, and therefore that there are circumstances where consent must be applicable even if the data controller is not seeking to rely on consent and the definition in Article 4(11) GDPR is not met. In the Complainant's view, this should result in a declaration that the data processing based on consent is unlawful for want of compliance with these "conditions of validity".

3.5 Facebook's position is that "[t]*he agreement to enter into a contract is a wholly separate matter to any form of consent to data processing…*",[17] and that:

> "*Article 4(11) GDPR is not relevant in this instance as Facebook Ireland is not seeking to rely on it (and the alternative legal basis sought to be relied on is valid). It is not the case that all types of processing must be assessed against the formal requirements under Article 4(11) GDPR. Indeed as the*

[13] Complainant Submissions on Final Report, page 16.
[14] *Ibid*, page 11.
[15] *Ibid*, page 40.
[16] *Ibid*.
[17] Submission 22 February 2019, paragraph 2.6.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

> *Draft Report acknowledges, consent is merely one of six possible bases upon which data processing may be legitimised under Article 6 GDPR. It is Facebook Ireland's position that an assessment against the formal requirements under Article 4(11) is only necessary and should only be undertaken where a controller purports to rely on consent. Put another way, where the controller relies on a different legal basis for a processing purpose, the analysis as to whether or not the processing is lawful should be undertaken in respect of the specific requirements for only that legal basis.*"

3.6 In light of this confirmation by the data controller that it does not seek to rely on consent in this context, there can be no dispute that, as a matter of fact, Facebook is not relying on consent as the lawful basis for the processing complained of. It has nonetheless been argued on the Complainant's behalf that Facebook *must* rely on consent, and that Facebook led the Complainant to believe that it was relying on consent. It should be acknowledged that Facebook relies on consent for some personal data processing activities on the platform, which users can provide or not provide through mechanisms distinct from the initial accepting of the Terms of Service.

3.7 The Investigator expressed the view that:

> "*…while the GDPR specifies that certain well-defined agreements as to processing (i.e. consent, as defined by the conditions set out in Article 4(11)) may legitimise processing under Article 6(1)(a), it does not expressly require that all agreements regarding processing must be legitimised on this basis.*"[18]

3.8 'Article 4 GDPR, as its title makes clear, sets out a series of definitions applicable under the GDPR as a whole. Article 4(11) GDPR merely defines consent for the purposes of the GDPR, including for the purpose of Article 6(1)(a) GDPR and Article 7 GDPR which sets out certain conditions for consent where it is being relied upon as the legal basis of processing. Article 4(11) GDPR does not, however, purport to determine the circumstances in which consent may be relied upon as a legal basis. While consent for the purposes of the GDPR must satisfy the definition in Article 4(11) GDPR, that provision does not in itself determine the circumstances in which consent may be relied upon as a legal basis for processing. Any other reading of Article 4(11) GDPR is not consistent with a systematic reading of the GDPR when it is clear that the legislator intended Article 4 GDPR to provide definitions. Other definitions, such as that of "controller", "processor", "main establishment" and "cross-border processing" are clearly just that: definitions. In any event, I am of the view that, in the context of this Complaint, this issue is an academic one. The key point for the purpose of this Draft Decision is that Facebook never sought to obtain consent from users through the clicking of "accept" to the Terms of Service.

[18] Final Report, paragraph 129.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

3.9 I put the views set out above to the Parties in the Preliminary Draft Decision. Facebook submitted that "*the Complainant's position is legally and factually wrong*" and that Facebook "*…does not seek to obtain consent to data processing from users when users are asked to contractually agree to its Terms of Service*".[19] Moreover, Facebook submits that it

> "*…did not request or require the data subject's consent to processing described in the Data Policy nor did it seek the data subject's consent to the processing described in, or otherwise performed for the purposes of, the Terms of Service, and as a consequence that the data subject did not in fact consent in this manner*".[20]

This confirms the position set out in the Preliminary Draft Decision: Facebook did not rely on consent as a legal basis for processing in this context. On this basis, Facebook expressed its agreement with the provisional finding that "*it is not legally obliged to rely on consent in order to deliver the Terms of Service and endorses the unequivocal decision of the Commission to reject the* [Complainant's] *argumen*t…".[21]

3.10 In contrast, the Complainant's submissions on the Preliminary Draft Decision argue that the alleged contract is an example of *falsa demonstratio* i.e. that Facebook has held out particular clauses as constituting part of a contract when, as a matter of law, they actually do not.[22] The Complainant in this regard relies on the perceived intention of the parties, the "*economic background and common understanding*", and the fact that the shift from reliance on consent to reliance on necessity for the performance of a contract was recent.

3.11 While this argument may be relevant in the context of reliance on Article 6(1)(b) GDPR – which is considered as the second issue below – it does not address the essential issue arising for the purposes of Article 6(1)(a) GDPR. In this case, Facebook is not relying on consent as a legal basis for processing of personal data under the Terms of Service. Indeed, the parties appear to agree that acceptance of the Terms of Service is not valid consent for the purposes of the GDPR.

3.12 For these reasons, I conclude that, as a matter of fact, Facebook did not rely, or purport to rely, on the Complainant's consent as a legal basis for the processing of personal data under the Terms of Service.

WHETHER THE CONTROLLER MUST RELY ON CONSENT

[19] Facebook Submissions on Preliminary Draft Decision, paragraph 1.7(B). See also paragraph 3.1
[20] *Ibid*, paragraph 3.1.
[21] Facebook Submissions on Preliminary Draft Decision, paragraph 4.1.
[22] *Ibid*, 4.4.1.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

3.13 Based on a new understanding of this issue that evolved during the course of this Inquiry, the Complainant made what I consider to be an alternative argument: namely, that Facebook was legally obliged to rely on consent and that, as Facebook has not done so, the processing was consequently unlawful.

3.14 In the Complainant's submissions on the Preliminary Draft Decision, it is denied that the Complainant advanced such an argument.[23] I have dealt with this point in part in footnote 36 of the Schedule. It remains the case that the Complainant has argued that where "*the subject matter of the declaration of intent…is primarily data processing*"[24] the appropriate legal basis must derive from Article 6(1)(a) GDPR, and where the subject matter of the contractual offer "*is primarily some other contractual service*",[25] the legal basis can derive from Article 6(1)(b) GDPR. In my view, it is difficult to interpret this as anything other than an argument that consent is the only appropriate legal basis for agreements primarily concerning data processing. This is, to put it another way, a suggestion that consent is a higher order of legal basis, at least in respect of agreements that primarily involve data processing. This being so, and for completeness, I will now consider whether consent under Article 6(1)(a) GDPR *must* be relied on by the controller in this context.

3.15 The Investigator points out that the Complaint begins by claiming that the data subject "*had to agree to*" Facebook's Terms of Service and Data Policy at the time of the update in April 2018.[26] In my view it is critically important to distinguish between agreeing to a contract (which may involve processing of personal data) and providing consent to personal data processing specifically for the purposes of legitimising that personal data processing under the GDPR. As noted by the EDPB, these are entirely distinct concepts which "*have different requirements and legal consequences*".[27] In particular, these are distinct legal bases for the processing of personal data under Article 6(1)(a) and 6(1)(b) GDPR, with all the consequences that this entails.

3.16 In this context, it is important to emphasise that GDPR does not set out any form of hierarchy of lawful bases that can be used for processing personal data, whether by reference to the categories of personal data or otherwise.[28] There is no question that "*one ground has normative priority over the others*".[29] This position is reflected in the Guidance of the Article 29 Working Party, which, although not legally binding, is nonetheless instructive in considering this

[23] Complainant Submissions on Preliminary Draft Decision, paragraph 4.4.2.
[24] Submissions on Draft Inquiry Report, page 35.
[25] *Ibid*.
[26] Final Report, paragraph 111, Complaint, Paragraph 1.3.
[27] 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, paragraph 17, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.
[28] C Kuner et al eds, *The EU General Data Protection Regulation: A Commentary* (Oxford 2020), page 329.
[29] *Ibid*.

issue.[30] I also note that, in the context of Directive 95/46/EC, which preceded the GDPR, the Court of Justice of the European Union ("the **CJEU**") has explicitly held that obtaining the data subject's consent is not a requirement for reliance on the "legitimate interests" legal basis.[31] The CJEU thereby rejected the argument that consent was a necessary legal basis in circumstances where the data controller sought to rely on another legal basis under Article 7 of the Directive. I have been pointed to no authority which supports the view that there is a particular lawful basis that is intrinsically preferable over others, or that one legal basis has legal primacy over any other, or that fulfilling one legal basis is a precondition for fulfilling a separate legal basis. In these circumstances, the reasoning of the CJEU in respect of Article 7 of Directive 95/46/EC is equally applicable to Article 6 GDPR. Indeed, notwithstanding the thrust of the argument initially advanced, the Complainant's submissions on the Preliminary Draft Decision now acknowledge that there is no hierarchy of legal bases under the GDPR.[32]

3.17 For this reason, if and insofar as it arises, I conclude that neither Article 6(1) GDPR nor any provision of the GDPR requires that the processing of personal data in particular contexts must necessarily be based on consent under Article 6(1)(a) GDPR.

3.18 In many cases involving a contract between a consumer and an organisation, the lawful basis for processing of personal data is "*necessity for the performance of a contract*" under Article 6(1)(b) GDPR. It cannot be said that the fact of agreeing to certain contractual terms – for example, by accepting the Terms of Service in this case – necessarily means that any processing of personal data under such contract is based on consent for the purposes of the GDPR. The question of whether a data controller can rely on Article 6(1)(b) GDPR turns on the terms of the particular contract, and whether the impugned processing operation(s) is/are necessary in order to bring about the performance of that contract. The nature and content of a contract freely entered into by two parties cannot, however, introduce a higher category of, or 'default', legal basis. Nothing in the GDPR supports the view that there is any such higher category or default legal basis.[33] I also note in this regard that the EDPB has advised that, in circumstances in which data processing is necessary to perform a contract, consent is not, in fact, an appropriate lawful basis on which to rely.[34]

3.19 I note, in this regard, that the Complainant has argued that a contract for a service with a social network "*primarily*" concerns data processing and on this basis should be based on

[30] Guidance 06/2014, page 10, at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[31] *Asociaţia de Proprietari bloc M5A-ScaraA v TK* Case 708/18, paragraph 41.
[32] Complainant Submissions on the Preliminary Draft Decision, paragraph 4.4.2.
[33] C Kuner et al eds, *The EU General Data Protection Regulation: A Commentary* (Oxford 2020), page 329.
[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, paragraph 17, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

consent.[35] At the same time, the Complainant asserts that the data processing in question is in fact not necessary for the performance of that same contract. I am unaware of any case-law or authority that suggest that companies cannot rely, at least in part, on Article 6(1)(b) GDPR as a legal basis for processing personal data simply because their businesses "*primarily*" concern data processing.

3.20 In truth, the Complainant's arguments in this respect appear to be made in support of the separate argument that Facebook cannot rely on Article 6(1)(b) as a lawful basis for processing. If the Complainant succeeds in that latter argument, it follows that another legal basis must be relied on and in this instance, in the Complainant's view, that legal basis would have to be consent. In my view, this alternative argument - to the effect that consent is the only remaining possible lawful basis because no other basis can be used lawfully for this particular agreement – is properly considered in the context of the second issue in the complaint, i.e. whether Facebook is entitled to rely on Article 6(1)(b) GDPR.

3.21 Finally, I note the Complainant's reliance on Article 7(2) GDPR, which states:

> "*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.*"

3.22 I also note the Complainant's reliance on Article 7(4) GDPR, which states:

> "*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 7 GDPR concerns 'conditions for consent' and is only relevant when considering where consent is being relied upon as the legal basis for processing in the first instance. This was the view of Advocate General Szpunar in *Planet49*.[36] Article 7 GDPR is not, in and of itself, indicative of which lawful basis a controller must or indeed should rely on in a particular context. Instead, where a controller is relying on consent, Article 7 GDPR assists in determining whether the

[35] Submissions on Draft Inquiry Report, page 35.
[36] Case 673/18 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V*, (Opinion of AG Szpunar) paragraph 97.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

'conditions for validity' (to use the Complainant's own language) have been met. As set out above, I have found that Facebook does not rely on consent in order to process data on foot of the Terms of Service, and also found that it is not legally required to do so. It follows that the argument relating to Article 7 GDPR is premised on a legal position that I have rejected.

3.24 I further note that the EDPB Guidelines on consent consider a number of circumstances in which "bundling" (or what the Complainant refers to as "forced consent" or "hidden consent") may occur. This occurs when consent can neither be freely given nor easily withdrawn because the provision of consent is made part of the terms of a contract, particularly in circumstances where there is an unequal balance of power between the data controller and the data subject.[37] This, however, only becomes relevant when the controller purports to rely on consent in the first place. For the reasons set out above, save in the case of limited additional processing activities (such as the use of facial recognition) above and beyond those based on the general Terms of Service, Facebook does not rely on consent and is not legally obliged to rely on consent. By its own admission, Facebook does not meet the definition of consent for the processing of personal data under the Terms of Service generally.

3.25 I have found that Facebook was not *prima facie* obliged to rely on Article 6(1)(a) GDPR to legitimise the processing arising out of this (or any) agreement, and moreover have found that as a matter of undisputed fact, Facebook did not rely on it. There is simply no persuasive authority in law that has been brought to my attention, or that I am aware of, for the proposition that any particular lawful basis in the GDPR can be "mandatory", "default" a "*lex specialis*", or of more or less significance than any other legal basis. In the absence of such authority, I am unable to accept the Complainant's arguments in respect of Issue 1. This being so, I reject the argument that the Complainant's clicking on the 'Accept' button in respect of Facebook's Terms of Service constitutes, or must be regarded as constituting, consent for the purposes of the GDPR.

3.26 Having considered the submissions of the parties, including the submissions on the Preliminary Draft Decision, I therefore conclude that the legal basis for processing of personal data under the Terms of Service between Facebook and its users, including the Complainant, does not, as a matter of law, have to be consent under Article 6(1)(a) GDPR and, as a matter of fact, Facebook does not rely on consent for this purpose and the agreement to the Terms of Service does not constitute consent for the purposes of the GDPR.

Finding 1:

Facebook has (a) 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.

[37] Guidelines 05/2020 on consent under Regulation 2016/679: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Pages 6-7.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

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

4.1 As set out above, the Complainant contends that Facebook's processing of personal data under the Terms of Service must be based entirely on consent as a legal basis under the GDPR. I have already found that this is not the case on the basis 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, as a matter of law, be based on consent. The Complainant's argument also rests on the contention that Facebook cannot rely on Article 6(1)(b) GDPR to process personal data in order to perform the Terms of Service.

4.2 In considering this issue, I will first address the relationship between the Terms of Service and the Data Policy. This assessment is necessary as the Complainant argues that she "agreed" to the Data Policy by accepting Facebook's updated Terms of Service. Facebook 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 Facebook 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 DATA POLICY

4.3 The Complainant alleges that in clicking the "accept" button, she agreed to both the Data Policy and the Terms of Service and that the alleged non-compliance is compounded by the agreement to both documents.[38] In examining this aspect of the Complaint, the Investigator was of the view that that the data subject's formal agreement to the Data Policy was not a component of the data subject's contract with Facebook. The Investigator also acknowledged in the Final Report that the Complainant seems to have conceded that there is no "consent" and therefore no "agreement" to the Data Policy.[39]

4.4 In respect of this matter, the Investigator concluded that, as Facebook has stated that the Terms of Service "*make up this entire agreement*" between Facebook and the Facebook user, there is no explicit indication, in the view of the Investigator, that Facebook intends the separate Data Policy to be part of that agreement. When Facebook sought agreement to the terms under dispute in this Inquiry, it invited users to also accept the updated Terms of Service and also included information on the Data Policy. In the Investigator's view, this illustrates that the Terms of Service and the Data Policy are entirely separate. Facebook's position is that the Data Policy is simply a compliance document setting out information required by the GDPR, whereas the contractual document is the Terms of Service.[40]

[38] Complaint, page 3.
[39] Final Report, paragraph 145.
[40] Facebook Submissions on Preliminary Draft Decision, paragraphs 5.5 - 5.6.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

4.5 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 Data Policy. I set out in detail when considering Issue 1 my reasons for concluding that no such consent in GDPR terms has taken place. I apply that reasoning to the current scenario. In my view, the acceptance in question is not an act of consent but, on its terms, constituted acceptance of, or agreement to, a contract i.e. the Terms of Service. Although the Data Policy was hyperlinked in the final stage of the engagement flow, I am not satisfied that the Data Policy was thereby incorporated into the Terms of Service. The "accept" button clearly referred to acceptance of the "terms" as distinct from the Data Policy (and indeed the Cookies Policy). In my view, the Data Policy is as Facebook has characterised it:

> "*While the Terms of Service list Facebook Ireland's services and obligations, the delivery and discharge of which require certain processing of personal data, they do not attempt to comprehensively list Facebook's Ireland's processing since the Data Policy does this and is the primary document to be considered when it comes to Facebook Ireland's GDPR obligations under Article 13. The distinct objectives and nature of these documents is further outlined in Sections 2 and 3 above where we have explained that agreement is merely sought to the Terms of Service but not for the Data Policy which functions as a transparency and not a contractual document.*"[41]

4.6 The Data Policy is a document through which Facebook seeks to comply with particular provisions of the GDPR in relation to transparency, whereas the Terms of Service is the contract between Facebook and its user. Facebook 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 the legal basis of contractual necessity is relied on, the contract in question is the Terms of Service. In my view, 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 Data Policy is only relevant insofar as it sheds light on the processing operations carried out for which Facebook relies on Article 6(1)(b) GDPR. It is essentially an explanatory document. After considering these views, which were set out in the Preliminary Draft Decision, Facebook expressed agreement with the provisional conclusions of the Commission in this regard.[42] The Complainant's submissions on the Preliminary Draft Decision did not express any further views on this issue.

4.7 The Data Policy itself references a very wide range of processing operations. As noted in the Schedule, the Complainant sought to direct the Commission to conduct an assessment of all processing operations carried out by Facebook. I have explained why it is not open to a Complainant – who must present a complaint with a reasonable degree of specificity – to demand such an assessment. While the Complaint refers to various examples of data processing, e.g. the processing of behavioural data, it does not go so far as to directly link the Complaint to specific

[41] Submissions on Draft Report, paragraph 7.1(A)
[42] *Ibid*.

processing operations by reference to an identifiable body of data with any great clarity or precision. In the circumstances, it is necessary to consider the issue relating to reliance on Article 6(1)(b) GDPR at the level of principle, and my findings are made on that basis.

4.8 More specifically, insofar as the Complaint refers to particular processing activities, it has a specific focus on data processed to facilitate behavioural advertising. This will accordingly be the focus of the analysis in this Draft Decision.

4.9 In order to ensure that this Inquiry has a reasonable degree of specificity, I will therefore consider whether Facebook can, in principle, rely on Article 6(1)(b) GDPR for processing under the contract, including and in particular in the context of behavioural advertising.

THE COMPLAINT, THE SUBMISSIONS OF THE PARTIES, AND THE REPORT

4.10 The Complainant argues that Facebook is not entitled to rely on Article 6(1)(b) GDPR, i.e. personal data processing that is necessary for the performance of a contract, as a legal basis. The Complainant contends that Facebook 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*".[43]

4.11 Specifically, the Complainant argues that the personalisation of posts and communication features constitutes a "core" element of Facebook's contract, but that personalised advertising does 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.

4.12 The Complainant takes issue with a lack of "differentiation" as between specific clauses or elements of the contract in the Commission's approach.[44] The Complainant argues that "*investigation*" and "*fact finding*" should have taken place in order to determine what specific

[43] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, page 16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[44] Complainant Submissions on Preliminary Draft Decision, paragraph 4.5.2.

elements of the contract are used by Facebook to justify specific processing operations. Firstly, it is clear from the Terms of Service, which is, in the Complainant's own words, a very descriptive document, that Facebook intends to provide behavioural advertising as part of its contractual service. While my view, as set out in Section 5 below, is that there have been significant failings of transparency in relation to this processing, that does not change this basic fact that behavioural advertising forms part of the service offered by Facebook. As noted above, the Complaint has a specific focus on behavioural advertising. On that basis, and having regard to the need for a reasonable degree of specificity in the presentation and investigation of complaints, it is not necessary to undertake a comprehensive investigation of each and every processing operation under the Terms of Service. I also emphasise, as I explain in further detail below, that I intend to order Facebook to bring its documents into compliance for transparency purposes. Such an order would vindicate the right of the Complainant and data subjects as a whole to get an answer to "*which specific clauses of the "Terms of Service" are used by Facebook to justify the specific purpose of its processing, the type of data processed, and the applicable legal basis*."[45] What such information would not do, is assist in deciding the question of principle as to whether Facebook can rely on Article 6(1)(b) GDPR in order to provide a service that includes behavioural or targeted advertising.

4.13 As a preliminary matter, I emphasise 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 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.

4.14 In this regard, I note that the Complainant explicitly sought to have the Commission investigate and make findings in respect of contract and consumer law. In the Preliminary Draft Decision I stated that I agree with the position of the Investigator that this falls outside the remit of a supervisory authority under the GDPR and is, in any case, the subject of both an Austrian consumer case against Facebook being pursued by Mr. Schrems, Honorary Chair of noyb, over the last 6 years,[46] and the *Bundeskartellamt* case being pursued by that office since 2016.[47] I further noted that the Investigator correctly drew the Complaint to the attention of the relevant Irish consumer and competition authorities, which have competence in this regard. I went on to observe that these legal regimes would be a more appropriate avenue for the Complainant to ventilate the issues surrounding contract law referred to above.

[45] *Ibid*.
[46] Mag. Maximilian Schrems v Facebook Ireland Limited, Case 3 Cg 52/14k-91, https://noyb.eu/sites/default/files/2020-06/Urteil%20FB_geschw%C3%A4rzt.pdf.
[47] See, for example, https://www.lexology.com/library/detail.aspx?g=abb936bc-8f3e-4f82-9266-2b3c591a2517.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

4.15 In the Complainant's submissions on the Preliminary Draft Decision, the Complainant took issue with these provisional conclusions. They were described as "*a perversion of justice*", "*an insult to any informed reader*", "*a cheap trick",* "*simply a lie*", "*(at best) too lazy*" and "*a wilful abuse of office*", all within the same fifteen lines of text.[48] The Commission rejects, in the strongest terms, these serious allegations of *mala fides*, dishonesty and otherwise illegal conduct. Such allegations go far beyond what is commonly encountered in even the most robustly argued set of submissions in an adversarial regulatory dispute. They have, moreover, been made without any foundation in fact or evidence and appear to be based solely on the fact that the there is a difference between noyb's interpretation of the law and the interpretation of the law set out in the Preliminary Draft Decision. The fact that the Complainant and/or the Complainant's representative have presented their arguments in this way is not conducive to the proper handling and investigation of Complaints and is to be regretted.

4.16 The Complainant argues that in order to determine the nature of the "agreement", it is necessary to fully inquire into the nature and scope of the agreement, and to apply Austrian contract law in so doing. In making this argument, the Complainant relies on a number of principles of contract law including Directive 93/13/EC ("the Unfair Terms Directive"). Reliance on the law of contract and on the Unfair Terms Directive is misplaced. If the Complainant contends that there is no contract, or that aspects of the Terms of Service do not constitute a lawfully formed contract or lawful and/or fair terms of the contract, it is open to her to pursue this matter before a relevant authority or before a court of law. The Commission is not empowered to make decisions as to the validity of contracts, be they consumer contracts or otherwise and, in particular, it has no jurisdiction whatsoever to make decisions in respect of Austrian contract law. The Commission is tasked with interpreting and applying the GDPR. Where the GDPR refers to a contract, the Commission cannot determine the interpretation and validity of such a contract for the purposes of the law more generally. The Commission is no more empowered to do this by law than it would be to declare processing based on compliance with a legal obligation under Article 6(1)(c) GDPR to be unlawful simply because a complainant would argue that the legal obligation being relied on was unconstitutional in their country. These are matters for the national courts or such other bodies as may be conferred with the jurisdiction to make such determinations under domestic law. Any such decision on the part of the Commission would be *ultra vires* the 2018 Act, for reasons explained in detail when I considered the extent of the Commission's powers earlier in this Draft Decision. I do not accept that this amounts to "*a denial of justice*",[49] for the reasons there set out.

4.17 The Complainant argues that the "Our Services" section of the Terms of Service "*are all neutral factual descriptions. Neither a duty of the user nor a service from Facebook results from the*

[48] Complainant Submissions on Preliminary Draft Decision, paragraph 4.5.1.
[49] *Ibid*.

wording".[50] The Complainant also argues that showing any user advertisements is a "*factual procedure*" rather than a contractual obligation or duty.[51] 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 "*compulsory consent*", i.e. consent which is made contingent on the acceptance of a contract.[52] 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 social network, and factual events simply mentioned or described in the contract i.e. showing advertisements.

4.18 As I have already found that there was no consent for the purposes of personal data processing under the GDPR, there therefore can be no "compulsory" consent associated with the acceptance of the contract. The remaining argument, however, is that this "take it or leave it" approach to signing up or continuing to use Facebook (to use the Complainant's terminology) in any event does not constitute processing that is permitted by Article 6(1)(b) GDPR. To assess whether the Complainant's 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 Facebook pursuant to the contract are necessary to fulfil the contract's core functions.

4.19 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 a social network",[53] the Complainant relies on guidance of the EDPB. Moreover, the Complainant argues that, *inter alia*, Facebook has made a "*ridiculous and impractical assertion that advertising (and similar secondary processing) is a core service.*"[54] The Complainant further argues that:

> "*Other elements which represent the core product of the platform (e.g. the user's page, exchange of news, contact book, photo uploads) are, according to the public opinion, certainly the subject of the product "social network" and thus the subject of the contract - irrespective of the designation in the clauses.*"

4.20 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 Facebook. The argument is that any services (such as, in the Complainant's view, advertising and "secondary processing") which do not form part of

[50] Submissions on Draft Report, paragraph 2.1.2
[51] *Ibid*, paragraph 2.1.7.
[52] *Ibid*, Paragraph 3.4.3.6.
[53] Complaint, page 4.
[54] Complainant Submission on Draft Report, paragraph 2.1.6.

the activities which are strictly necessary to fulfil the core objective of the contract cannot be rendered lawful by Article 6(1)(b) GDPR.

4.21 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, Facebook 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. Facebook argues that it is entitled to rely on Article 6(1)(b) GDPR to deliver services in a contract even if that processing is not the most minimal processing available to it in order to deliver the service being provided.

4.22 Facebook argues that there is no basis to contend that Facebook, in clearly relying on a contract with the user, has attempted to mislead the user and to "infer" consent from a user. Facebook's position is that the condition of necessity for contractual performance "*does not mean that processing must be essential to the performance of the contract, or the only way to perform the underlying contract*".[55] Facebook 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. Facebook's position is therefore that the Complainant's interpretation (and proposed application) of the GDPR is incorrect and excessively narrow, insofar as the contract between Facebook and its users are concerned.

4.23 Facebook 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 "*Article 6(1)(b) forms part of the right to data protection, it is not a derogation or limitation on the right. It operates as a safeguard by explaining the circumstances in which the personal data can be processed*".[56] Facebook's position is that the Commission should apply a broader interpretation of Article 6(1)(b) GDPR, such that processing 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 relation to targeted behavioural advertising specifically, Facebook argues that:

> "*Beyond ensuring the continued financing of the provision and development of the Service, which is itself of significant benefit to users (as the Complaint explicitly recognises), the data processing activities undertaken by Facebook Ireland primarily enable Facebook Ireland to*

[55] Submissions on Draft Report, paragraph 4.2.
[56] Submission on Draft Report 29 July 2019, paragraph 4.2.

> *provide its personalised services to users (including curating individual's News Feed, the content they see, connections suggested, advertising and other commercial content, shortcuts suggested and elements of the features they can enjoy). This is itself the core of the Service and one of the principal reasons why users value the Service over and above the services provided by Facebook Ireland's competitors*."[57]

4.24 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.[58] 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.[59] 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.*".[60].

4.25 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 FACEBOOK CAN RELY ON ARTICLE 6(1)(B) GDPR

4.26 In coming to a conclusion on this matter in the Preliminary Draft Decision, 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 and address this issue in general terms, they 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*".[61] 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 and the application of these concepts to the specific contract relied upon for the purposes of Article 6(1)(b) GDPR. This remains my view in the context of this Draft Decision.

[57] Submissions on Draft Report, paragraph 1.4.
[58] Final Report, page 47.
[59] *Ibid*, page 48.
[60] *Ibid*, paragraph 203.
[61] 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-b-adopted_after_public_consultation_en.pdf, paragraph 22.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

4.27 It is, in my view, important to have regard not just to the concept of what is "necessary", but also to the concept of "performance". The EDPB has stated that the controller should ensure "*that processing is necessary in order that the particular contract with the data subject can be performed.*"[62] A contract is performed when each party discharges their contractual 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 subject-matter 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*".[63] It remains the case however that necessity cannot be considered entirely in the abstract, and careful regard must be had for what is necessary for the performance of the specific contract freely entered into by the parties.

4.28 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].[64]

4.29 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.*"[65]

4.30 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.[66] 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*

[62] *Ibid*, paragraph 26.
[63] *Ibid*, paragraph 30.
[64] Guidelines 2/2019, paragraph 27.
[65] *Ibid*, paragraph 30.
[66] *Ibid*, paragraph 23.

directive".[67] It is important to highlight, as the Investigator has,[68] that in the same case the 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".[69] 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).*"[70]

4.31 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 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 is necessary to fulfil the "*specific*"[71] or "*particular*"[72] 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.

4.32 In accordance with the EDPB Guidelines, 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, 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 "a social network" in a general sense, but what is necessary to fulfil the core functions of the particular contract between Facebook and Facebook users. In order to carry out this assessment, it is therefore necessary to consider the contract itself.

4.33 I recall my earlier statement that matters of national contract law are outside the scope of the Commission.[73] 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*".[74] In my view, when examining what constitutes a "contract" for the

[67] Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 18 December 2008, para. 52.
[68] Final Report, paragraph 202(vi).
[69] *Huber v Deutschland*, paragraph 62.
[70] Guidelines 2/2019, paragraph 27.
[71] *Ibid*, paragraph 30.
[72] *Ibid*, paragraph 26.
[73] 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.
[74] 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-b-adopted_after_public_consultation_en.pdf, paragraph 30.

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.

4.34 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?*"[75]

4.35 In considering this particular issue in the context of the Complaint, it is necessary to identify the "core" functions of the contract between Facebook and Facebook 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 is not necessary for the purposes of performing the Terms of Service. The Complainant has however made extensive submissions arguing that the serving of behavioural advertising specifically is not necessary in order to fulfil the "core function" of a social network. As a result, for the purposes of this Complaint, I propose to focus on this element of the Terms of Service.

4.36 The contract between Facebook and Facebook users is divided into the following headings:

- "To Provide a Personalised Experience for you";
- "Connect you with people and organizations you care about";
- "Empower you to express yourself and communicate about what matters to you";
- "Help you discover content, products, and services that may interest you";
- "Combat harmful conduct and protect and support our community";
- "Use and develop advanced technologies to provide safe and functional services for everyone"; and
- "Enable global access to our services".

[75] *Ibid*, paragraph 33.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

4.37 The first term in the Terms of Service, under the heading "To Provide a Personalised Experience for you", states that:

> "*from the posts, stories, events, ads, and other content you see in News Feed or our video platform to the Pages you follow and other features you might use, such as Trending, Marketplace, and search. We use the data we have – for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products – to personalize your experience*" [my emphasis].

4.38 As well as the provision relating to advertisements at the beginning of the Terms of Service already set out, I note that under the heading "*Help you discover content, products, and services that may interest you*", the contract states "[w]*e show you ads, offers and other sponsored content to help you to discover content, products and services*…".

4.39 The Complainant however argues that such advertising referred to in this term is not necessary in order to deliver a social network, and that simply placing these terms in the contract does not make them necessary. Both of these statements may be true, but it does not follow that fulfilling these terms is not necessary in order to fulfil the specific contract with Facebook. 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*". Facebook's argument is essentially that personalised advertising constitutes the "*core*" of its service, and would therefore be the Facebook service's "*distinguishing characteristics*" (to use the language of the EDPB).[76] The Facebook service is clearly "*promoted* [and] *advertised*"[77] as being one that provides personalised advertisements, and in my view, a reasonable user would be well-informed, based on public debate of these issues in the media among other matters, that this is the very nature of the service being offered by Facebook and contained within the contract.

4.40 However, the position of the Complainant 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:

> "*as a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services. Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads. This is all the more supported by the fact that data subjects have*

[76] *Ibid*, paragraph 33.
[77] *Ibid*.

the absolute right under Article 21 to object to processing of their data for direct marketing purposes."[78]

4.41 The Guidelines, while not binding on the Commission, 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 personalised advertising as an example of processing that will usually not be necessary. As the terms of the guidance makes clear, this is, however, a general rather than an absolute rule. I note the EDPB has also acknowledged that "*personalisation of content may (but does not always) constitute an essential or expected element of certain online services*".[79] The core area of dispute in applying Article 6(1)(b) GDPR is therefore whether – by reference to the terms of the specific contract - the inclusion of behavioural advertising makes data processing conditional on the delivery of a contract, where that processing is not itself necessary to actually deliver the contract. The counter-argument is that such advertising, being the core of Facebook's business model and the core of the bargain being struck by Facebook users and Facebook, is necessary to perform the specific contract between Facebook and the Complainant.

4.42 Appling the principles set out above to the particular circumstances of this case, it seems to be that the core of the Facebook model, particularly in circumstances where users do not pay for the service, is an advertising model.[80] 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*".[81] The core of the service, however, as set out in the specific contract with the data subject in this case, clearly includes (and indeed appears to be premised upon) the provision of personalised advertising.

4.43 This analysis is reinforced when one answers the specific questions posed at paragraph 33 of the EDPB Guidelines set out above. The nature of the service being offered to Facebook users is set out in the first line of the Terms of Service: a personalised service that includes advertising. Moreover, a distinguishing feature of the Facebook service (that, I think it might be fair to say, the Complainant and Facebook would both agree on) is that it is a service funded by personalised advertising. As the core of the bargain between the parties, this advertising therefore appears to be part of the substance and fundamental object of the contract. It is, in fact, the core element of the commercial transaction as between Facebook and Facebook users. It follows that this is a commercially essential element of the contract. As this information is both clearly set out and publicly available, it is difficult to argue that this is not part of the mutual expectations of a prospective user and of Facebook. Finally, it is clear that the service is advertised (and widely understood) as one funded by personalised advertising, and so any reasonable user would expect

[78] *Ibid*, paragraph 52 (emphasis added).
[79] *Ibid*, paragraph 54.
[80] E.g. Facebook Submissions on the Draft Report, paragraph 6.3(C) and Facebook Submissions on Preliminary Draft Decision, paragraph 5.8(C).
[81] *Ibid*, paragraph 36.

and understand that this was the bargain being struck, even if they might prefer that the market would offer them better alternative choices. I am therefore of the view that the answers to the questions proposed by the EDPB do not support the Complainant's argument in respect of Article 6(1)(b) GDPR in the context of the contract concluded between Facebook and the Complainant at issue in this Complaint.

4.44 In the submissions on the Preliminary Draft Decision, the Complainant argues that this analysis amounts to speculation.[82] While making the argument that the legal analysis must be based on "*hard evidence*" rather than "*views*", the only evidence put forward by the Complainant is her own statement and a Gallup poll referenced in the Complaint. The Complainant goes on to suggest that "*we might as well ask the Oracle of Delphi what data subjects really know or think and what economics really play out in a contractual relationship*."[83] While I have had due regard to the matters put forward by the Complainant in support of the Complaint, in reaching my conclusion, I am obliged to consider all of the evidence before me and I am also entitled to take notice of matters in the public domain. In any event, in this specific context, it is primarily by reference to the contract itself that the question of reliance on Article 6(1)(b) GDPR must be assessed. Having regard to the clear terms of the contract, targeted advertising forms a core element of Facebook's business model and transaction with users.

4.45 The Complainant's submissions on the Preliminary Draft Decision go on to describe the "*data for service narrative*" as "*economically illiterate*", "*clearly way too simplistic*", "*deeply alarming*" and an "*ancient industry lobbyist narrative*".[84] In support of these assertions, it is argued that each visit to Facebook involves spending time, "*the most important online currency on Facebook*". The submissions further argue that Facebook can only profit from advertising because users provide relevant content to other users with no remuneration.

4.46 The fact that a user spending additional time on a platform is more lucrative for Facebook does nothing to rebut the argument that targeted advertising lies at the core of the agreement. The more time a user spends engaging with the platform, the more advertisements they will be exposed to and the more data they will provide. Indeed, even if one uncritically accepts this argument, it may be regarded as reinforcing the conclusion that the core of the business model is the provision of data on personal activity to facilitate targeted advertising. The fact that intra-user activity enables profit does not alter where those profits come from, or the nature of the agreement and what is necessary in order to perform it. It is clear that the Complainant regards this state of affairs as being unfair and/or unbalanced. Whether it is or it is not, this does not alter the fact that the service in question is provided to users on this very basis.

[82] Complainant Submissions on Preliminary Draft Decision, paragraph 4.5.3.
[83] *Ibid*.
[84] *Ibid*.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

4.47 I have already pointed out that the Guidelines are non-binding and do not determine the application of the general principles to specific cases. I agree with the majority of the arguments of both the Complainant and the EDPB in relation to the correct interpretation of Article 6(1)(b) GDPR.[85] However, I have difficulty with a strict threshold of "impossibility" in the assessment of necessity. By "impossibility", I am referring to the argument put forward that a particular term of a contract (here, behavioural advertising) is not necessary to deliver an overall service or contract. In particular, I consider that is not correct to assess necessity as against the delivery of an overall service in the abstract. Rather, as I have stated above, I consider the appropriate assessment to be one which considers what is necessary by reference to core function of the particular contract.

4.48 While I accept that either form of assessment will require an element of reasoning in the abstract (in particular, when considering the mutual perspectives and expectations), 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 the performance of a contract possible or impossible. Instead, the general principles set out in the GDPR and explained by the EDPB in the Guidance must be applied. These principles must be applied on a case-by-case basis. While the examples provided in the EDPB Guidance are helpful and instructive, they are not conclusive of the position in any specific case and indeed do not purport to be.

4.49 Even if, contrary to my conclusion, the appropriate standard in assessing Article 6(1)(b) GDPR was one of impossibility rather than necessity *simpliciter*, Facebook has submitted that "…*it would be impossible to provide the Facebook service in accordance with the Terms of Service without providing personalised advertising*".[86] While it does not consider that this would be the correct interpretation of the law, it considers that this standard would nonetheless be met under the Terms of Service.

4.50 While I remain of the view that Article 6(1)(b) GDPR cannot be interpreted as meaning that, unless it is impossible to perform the contract without particular acts or operations of data processing, such processing is not necessary for the performance of the contract, this argument underlines the extent to which targeted advertising forms a core part of the contract between Facebook and its user.

4.51 Based on the above considerations, I conclude that neither Article 6(1)(b) nor any other provision of the GPDR precludes Facebook from relying on Article 6(1)(b) GDPR as a legal basis to for the delivery of a service based on behavioural advertising of the kind provided for under the contract between Facebook and its users at issue in this Complaint. As discussed below, other provisions of the GDPR (such as transparency, which I consider at Issue 3) act to strictly regulate

[85] While in the submissions on the Preliminary Draft Decision the Complainant takes issue with my approach to the EDPB Guidelines, the Complainant has made no additional arguments beyond those already set out about why this legally cannot or should not be done: Complainant Submissions on the Preliminary Draft Decision, paragraph 4.5.5.
[86] *Ibid*, paragraph 5.8(G).

the manner in which this service is to be delivered, and the information that should be given to users.

4.52 Having analysed the submissions of the parties, the terms of the GDPR, and the jurisprudence and EDPB Guidelines, I find no basis for the contention that Facebook 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 behavioural advertising insofar as that forms a core part of the service. There is nothing in the GDPR that 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 analysis, the data may be processed if, without such processing, the contract could not be performed. I am not convinced, for the reasons set out, that Article 6(1)(b) GDPR goes a step further and excludes all processing unless the fulfilment of some abstractly discerned purpose would be rendered impossible without that processing. I am also of the view that this application conforms broadly to significant elements of the interpretation of Article 6(1)(b) GDPR proposed by the Complainant and by the EDPB.

4.53 While I accept that, as a general rule, the EPDB considers that processing for online behavioural advertising would not be necessary for the performance 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 conclude that Facebook may in principle rely on Article 6(1)(b) as a legal basis of the processing of users' data necessary for the provision of its service, including through the provision of behavioural advertising insofar as this forms a core part of that service offered to and accepted by users.

4.54 Having regard to the scope of the Complaint and this Inquiry, as described above, this is not to be construed as an indication that all processing operations carried out on users' personal data are necessarily covered by Article 6(1)(b) GDPR.

4.55 I therefore find that Facebook is, in principle, entitled to rely on Article 6(1)(b) GDPR as a legal basis for the processing of a user's data necessary for the provision of its service, including through the provision of behavioural advertising insofar as this forms a core part of that service offered to and accepted by the user under the contract between Facebook and its user.

Finding 2:
I find the Complainant's case is not made out that the GDPR does not permit the reliance by Facebook on 6(1)(b) GDPR in the context of its offering of Terms of Service.

5 ISSUE 3 – WHETHER FACEBOOK 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

5.1 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');*
>
> *(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').*"

5.2 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.*"

5.3 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.*"

5.4 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.*"

5.5 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.*"[87]

5.6 In the Complaint, the Complainant alleges that Facebook'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.[88] The Investigator therefore examined whether it could be alleged that the Complainant was led to believe this was the case.

5.7 The Complainant argues that there was a lack of clarity in respect of the data processing which was carried out on foot of the alleged "forced consent" to the Terms of Service. Indeed, the Complaint

[87] 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.
[88] Complaint, page 3.

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).*"[89] Furthermore, the Complainant argues 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*."

5.8 The Complainant asserts that the clicking of "accept" on the Terms of Service generated the belief that the processing was based on consent. In my view, this is surprising, given the common nature of such "click wrap" contractual agreements utilised by most, if not all, online platforms. Nonetheless, the Complainant outlined and provided the Commission with an affidavit (sworn statement) sworn by the data subject, which stated that the "overall impression" created by the "accept" button was that the data subject was providing their consent within the meaning of Article 6(1)(a) GDPR. It is stated that the data subject did not read the Legal Basis Information Page prior to agreeing to the Terms of Service. The Complainant raised a number of other additional points relating to the engagement flow, including its design, which according to the Complainant was intended to cause "user fatigue" and also an alleged difficulty in navigating to the Legal Basis Information Page.

5.9 In this way, inherent in this Complaint is the argument that the legal basis relied on by Facebook 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 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 sets out that this information required by 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.

5.10 Given the Complaint's focus on the alleged "forced consent" and on processing carried out on foot of the acceptance of the Terms of Service, I will confine the transparency analysis in the Preliminary Draft Decision to questions relating to information on the lawful basis for processing data arising from that acceptance. It follows that, as well as Article 5(1)(a) GDPR, Article 13(1)(c) GPDR must be considered, as well as the accompanying requirement that the information required by that latter

[89] *Ibid*. paragraph 2.3.1.

provision be set out in accordance with Article 12(1) GDPR. As I have already found that, to the extent specific processing operations are complained of, the processing is based on Article 6(1)(b) GDPR, the central focus of the Preliminary Draft Decision in respect of this issue is compliance with Article 13(1)(c) GDPR to the context of that lawful basis.

5.11 In its submissions on the Draft Report, the Complainant further detailed its objections in relation to transparency by arguing that "*there is also no clear statement which data are processed for which purposes under the legal basis of Article 6(1)(b) GDPR*",[90] and that "[t]*he only document Facebook puts forward to prove the complainant's alleged information about the alleged change of legal basis is the hard-to-find sub-sub-page on "legal basis", which is anything but an easily accessible form*".[91]

THE "LAYERED" APPROACH

5.12 I have already set out the reasons for my disagreement with the Investigator's use of a distinction between the question of whether the data subject was misled and the broader question of whether the Data Policy complies with the transparency provisions of the GDPR. The obligation for a controller to comply with these transparency provisions constitute, in and of themselves, the entirety of the Complainant's right not to be misled under the GDPR.

5.13 When the Investigator considered compliance with the transparency requirements in this context, he adopted a "layered" approach. That is to say, each "layer" of the documents in question were assessed in isolation for their individual compliance before a final "cumulative" view was expressed. Facebook disagreed with this approach, arguing that "[t]*he GDPR contains no such concept of distinct layers and does not require a layered approach. Controllers are obliged to take appropriate measures to provide information to data subjects and are permitted to achieve this in ways they consider appropriate*".[92]

5.14 The Investigator disagreed with Facebook's submissions, and expressed the view that:

> "*in order to assess the layered provision of information, it is first necessary to consider the discrete information sources separately, in order to arrive at an overall view. Accordingly, the following assessment of primary, secondary and tertiary sources of information provided by Facebook is not premised on "separatist approach", rather, it constitutes a comprehensive assessment of the manner in which information has been provided to the data subject. The investigator also considers that, where a controller adopts a layered approach to the provision of*

[90] Submissions on Final Report, paragraph 2.4.1.3.
[91] *Ibid*, paragraph 3.4.3.1.1.
[92] Submissions 22 February 2019, paragraph 5.9.

information, each layer must comply independently with the requirement of Article 12(1) GDPR regarding the provision of information".[93]

5.15 I respectfully disagree with the premise of the Investigator's reasons for adopting this approach. Article 12(1) GDPR is directed to ensuring, insofar as possible, that the data subject receives the information that is "provided" by the data controller. It does this by reference to the potential barriers that could operate to prevent the information from being received by the data subject. The requirement, for example, for the data controller to use "clear and plain language" when "providing" the information helps to ensure that the data subject is not hindered in receiving the information because of an inability to understand complicated or technical jargon. Similarly, the requirement for the data controller to "provide" the information in a "concise" manner helps to ensure that the data subject is not hindered in receiving the information as a result of information fatigue caused by the incorporation of the information into a long and rambling piece of text.

5.16 Article 12(1) GDPR, however, clearly deals with "*any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34*" [my emphasis]. Therefore, compliance with this provision can only be assessed by reference to the provision of information mandated by Articles 13 and 14 GDPR as appropriate; it is not a requirement applied generally to every single piece of information provided to the data subject concerning data processing. There is no requirement that the information mandated by Article 13(1)(c) GDPR be contained in any particular "layer" of information; there is simply a requirement that the information be provided, and that the information be set out in the manner required by Article 12(1) GDPR. Therefore, each individual "layer" cannot be assessed by reference to Article 12(1) GDPR independently of the information required by Article 13(1)(c) GDPR.

5.17 Given that a controller is free to choose not to put particular information in a particular layer, it must follow that Article 12(1) GDPR cannot be used as a basis for assessing each layer independently. It may well be the case that something about the "layered" approach taken by a controller could ultimately mean the information required by Article 13(1)(c) GDPR is not set out in the manner required by Article 12(1) GDPR. That in itself, however, is not a justification for an isolated and/or abstract assessment of each individual layer, without reference to other layers, for compliance with Article 12(1) GDPR. On that basis, while the Investigator's view on the issue of infringements was expressed by reference to each individual layer before finally arriving at a separate view in relation to the documents as a whole, I propose to approach the assessment strictly by reference to the requirements of Articles 12(1) and 13(1)(c) GDPR. Once the information has been provided and has been provided in a compliant manner, it does not matter whether a controller has achieved the objective by the use of layering, nor does it matter what precisely is contained in each layer.

5.18 For the avoidance of doubt, I am not expressing any particular view on the merits or otherwise of controllers adopting a layered approach. Moreover, I am conscious that a layered approach for the

[93] Final Report, paragraphs 297-298.

provision of information on online services has been explicitly endorsed by the Article 29 Working Party Guidelines (and, in turn, endorsed by the EDPB).[94] I am instead expressing a view on the appropriate manner in which to assess the compliance of any such layered information with Articles 12 and 13 GDPR. In my view, while the Investigator's analysis was robust and comprehensive, the consideration of the documents was not sufficiently holistic, insofar as individual layers were initially assessed for compliance without reference to the information or documents as a whole.

5.19 In addition, I should add that a cumulative assessment of the information provided and the manner in which the information is provided must always be carried out, irrespective of whether the Investigator was correct to also assess each layer individually, or whether Facebook was correct to argue that the individual layers should not be considered in this manner. In circumstances where the layered documents, when considered cumulatively, lack the information required by Article 13 GDPR or are not set out in a manner compliant with Article 12 GDPR, it matters not whether any individual layer is deficient or otherwise; there would still be an infringement of the provision.

5.20 The Investigator was of the general view that the "Legal Basis Information Page" (a term used by the Investigator for an unnamed page linked to the Data Policy and Terms of Service) is transparent about Facebook's reliance on Article 6(1)(b) GDPR, and that therefore it was transparent that data would be processed on that basis arising out of acceptance of the Terms of Service.[95] The Investigator went on to express a number of views to the effect that Articles 12(1) and 13(1)(c) GDPR were being infringed on the basis that each "layer" of information failed to set out specific processing operations (or sets of operations), their individual purpose, and the lawful basis being relied on for each. Facebook's position is that Article 13(1)(c) GDPR "*does not require a controller to provide this information in relation to specific processing operations, rather, it requires transparency in relation to the processing purposes.*"[96] Facebook further argues that the definition of "processing" in Article 4(2) GDPR, i.e. an "operation or sets of operations", cannot be used to circumvent, what they say is, the clear intention of the legislator to use the term "processing" instead of "processing operations", when the latter appears in the text of the GDPR over fifty times.[97] I consider this argument in more detail below.

5.21 Many of the points of dispute that characterise the submissions of Facebook on the Draft Report and the contents of the Final Report relate to the dispute as to the appropriateness of assessing compliance with reference to each individual "layer" of information. I have set out my view in that regard already. I also note that, in its submissions on the Preliminary Draft Decision, Facebook expressed agreement with this conclusion, and maintained that the relevant consideration "*is whether, cumulatively, the data subject has been provided with the information required under the GDPR.*"[98]

[94] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018.
[95] Final Report, Paragraph 256.
[96] Submissions of 22 February 2019, paragraph 2.2.
[97] Submissions on the Draft Report (September 2019), paragraph 5.5.
[98] Submissions on the Preliminary Draft Decision, paragraph 7.1.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

Therefore I will now proceed to consider whether, in my view, Facebook has been transparent with the Complainant (and therefore with data subjects in general) in relation to processing for which it relies on Article 6(1)(b) GDPR. I will make further reference to the Reports, and the submissions of the parties when considering that issue.

THE EXTENT OF THE OBLIGATION IN ARTICLE 13(1)(C) GDPR

5.22 In the Investigator's view, Article 13(1)(c) requires a data controller to set out a description of the processing operation or sets of operations undertaken by the controller to fulfil that purpose, and the legal basis relied on by the controller in order to carry out that processing operation or sets of operations. His view is that "*the obligation under Article 13(1)(c) requires the provision of two types of information to the data subject: (i) information which specifies the lawful basis for processing , and (ii) information which describes the processing associated with that lawful basis*".[99] Facebook's view on the matter is that there is no such specific obligation for "*the legal basis being mapped to the purpose of processing*".[100] Facebook argues that the legal bases and purposes can be set out in a manner that does not necessarily link one to the other.

5.23 Article 4(2) GDPR, which deals with interpretation, states that:

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

5.24 I also note that Recital 60 states that "*principles of fair and transparent processing require that the data subject be informed of the <u>existence of the processing operation and its purposes</u>*". The Article 29 Working Party has opined that:

> "*Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject. Connected to this, the accountability principle requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR.*"[101]

[99] Final Report, paragraph 283.
[100] Submissions on the Final Report, paragraph 5.13.
[101] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

5.25 Facebook has sought to argue that the absence of a specific reference to processing "operation" in Article 13(1)(c) GDPR means that the obligation to provide information to data subjects does not necessitate an approach whereby the prescribed information is provided by reference to individual processing operation(s). In the Preliminary Draft Decision, I did not agree with this position. The Preliminary Draft Decision set out that Article 4(2) GDPR clearly identifies that the definitions set out in that provision are "for the purposes of" the GDPR and that there is no limitation on the application of the prescribed definitions, either within Article 4 GDPR or in the context of other individual provisions of the Regulation. For this reason, the Preliminary Draft Decision expressed the view that an argument premised on a suggestion that the definition of "processing" should only be applied to those provisions that incorporate specific reference, within its own text, to an "operation" or "operations", was legally unsustainable based on a literal interpretation of the GDPR.

5.26 I note that the Investigator agreed with Facebook's argument that Article 13(1)(c) GDPR requires a data controller to provide information in relation to the purpose(s) of the processing in conjunction with the corresponding legal basis for processing. However, the phrase "*for which the personal data were intended*", suggests that the data controller should also provide this information in such a way that enables the data subject to understand which personal data are/will be processed, for what processing operation and by reference to which legal basis, at least in broad terms.

5.27 In expressing disagreement with the proposed literal interpretation of Article 13(1)(c) GDPR set out in the Preliminary Draft Decision, Facebook submitted that "*Facebook Ireland's interpretation directly tracks the actual wording of the relevant GDPR provision which stipulates only that two items of information be provided about the processing (i.e. purposes and legal bases). It says nothing about processing operations.*"[102] Facebook submitted that because, in its view, Article 13(1) GDPR applies "*at the time data is collected*", and therefore refers only to "*prospective processing*". It submits that, on this basis, Article 13(1)(c) GDPR does not relate to ongoing processing operations, but is concerned solely with information on "*intended processing*".[103] Facebook's position is therefore that Article 13(1)(c) GDPR is future-gazing or prospective only in its application and that such an interpretation is supported by a literal reading of the GDPR.

5.28 Facebook argues that, despite the provision of a clear definition of "processing" in Article 4(2) GDPR, Article 13(1)(c) GDPR sets out:

> "*only two specific features of the processing that need to be provided. Article 13(1)(c) GDPR does not require disclosure, for example, of various other aspects of processing referenced in Article 4(2) GDPR, namely, the intended nature of the processing, or the intended form in which the data will be processed, or the intended duration of the processing, which is*

[102] Submissions on the Preliminary Draft Decision, paragraph 8.2(A).
[103] *Ibid*, paragraph 8.2(B).

> *separately required and addressed by Article 13(2)(a) GDPR. Similarly, another aspect of processing – namely, the identity of any recipient – is explicitly included under Article 13(1)(e) GDPR, but the same is not done as regards the specifying of processing operations. As such, the generic definition of "processing" in Article 4(2) GDPR is not relevant to the analysis of what Article 13(1)(c) GDPR requires."*[104]

5.29 Facebook's argument above is premised on the suggestion that the various provisions of Article 13 GDPR require the disclosure to data subjects of specific aspects of the broader activity or "processing" as defined by Article 4(2) GDPR, such as the identity of a recipient, the duration of the processing, etc. Facebook makes the point that nothing in Article 13 requires them to specify if storage, transmission or dissemination, for example, are the *forms* of processing engaged. That is correct. However, what Article 13 does clearly require is that the purposes and legal bases must be specified in respect of the *intended processing*. Purposes and legal bases cannot simply be cited in the abstract and detached from the personal data processing they concern.

5.30 As Facebook's position cannot be reconciled with a literal reading of the GDPR, for completeness, it is necessary to consider whether its position is nonetheless justified by a systemic reading based on the legislator's objective and the contents of the GDPR as a whole. Firstly in relation to the argument I have just dealt with, it is important to note that transparency, both under the GDPR and in the Guidelines that are to be considered in this Draft Decision, are directly linked to the principle of accountability under the GDPR. In order to ensure that actual or intended processing is carried out in an accountable and transparent manner, the interpretation proposed by Facebook cannot be accepted. Firstly, the absence of any level of specificity as to what the data controller is doing with the data, and more fundamentally what data they are processing at all, would render information on the purposes of this unspecified processing almost useless to a data subject. In the absence of information on the nature of the data being used and the nature of the processing being carried out, it would be nigh on impossible to exercise data subject rights in an informed manner. Such an absence of transparency and accountability could not be reconciled with a purposive or systematic reading of the GDPR.

5.31 Facebook goes on to provide examples of previous drafts of the GDPR where the legislator considered requiring additional material in Article 13 GDPR, including "*the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk*".[105] The decision of the legislator not to include a requirement to provide such information has no impact on the applicability of the clear definition of "processing" in Article 4(2) GDPR, and therefore does not affect the appropriate literal interpretation of Article 13(1)(c) GDPR. In any purposive or systematic approach to interpreting the provision, the decision not to require information on processing which the controller itself has found to be high risk does not suggest that

[104] *Ibid*, paragraph 8.2(C).
[105] *Ibid*, paragraph 8.2(E).

the controller would not otherwise be required to disclose the existence of that processing. It would simply require a controller to disclose that a data protection impact assessment indicated the presence of a high risk. This therefore provides no evidence that the legislator excluded in any way the interpretation of Article 13(1)(c) GDPR being proposed.

5.32 Article 5(1)(b) GDPR states that personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*", and Article 5(1)(c) GDPR states that the data shall be "*limited to what is necessary in relation to the purposes for which they are processed*" [emphasis added]. The core principles clearly focus quite closely on the purposes for processing (defined, by Article 4(11) GDPR, as "processing operations or sets of operations). While Article 5 GDPR lays down six different principles, those principles are interconnected and operate, in combination, to underpin the GDPR as a whole.

5.33 Considering the purpose limitation principle, I note that this principle identifies the obligations which arise by reference to the terms "collection" and "further" processing. This is very similar to the language of Article 13(1)(c) GDPR, as the introductory passage to Article 13 GDPR contains a reference to "collection", and Article 13(1)(c) GDPR itself refers to "*the purposes of the processing for which the personal data are intended*". It therefore can be said that Article 13 GDPR also considers "collection" and "further" processing. For this reason, it is useful to examine further the requirements and function of the purpose limitation principle enshrined in Article 5(1)(b) GDPR.

5.34 The Article 29 Working Party has provided Guidance that states:

> "*When setting out the requirement of compatibility, the Directive does not specifically refer to processing for the 'originally specified purposes' and processing for 'purposes defined subsequently'. Rather, it differentiates between the very first processing operation, which is collection, and all other subsequent processing operations (including for instance the very first typical processing operation following collection – the storage of data).*
>
> *In other words: any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility*"

5.35 This introduces a distinction between "purpose specification" and "compatible use". In relation to specifying the purpose for which data is collected, the Article 29 Working Party stated that:

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

> "[P]*ersonal data should only be collected for 'specified, explicit and legitimate' purposes. Data are collected for certain aims; these aims are the 'raison d'être' of the processing operations. As a prerequisite for other data quality requirements, purpose specification will determine the relevant data to be collected, retention periods, and all other key aspects of how personal data will be processed for the chosen purpose/s.*"

5.36 In considering the purpose limitation principle, i.e. compatible use, it was set out that:

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

5.37 It was further stated that:

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

5.38 The Article 29 Working Party also emphasised the benefits to the data subject from such transparency and accountability, by enabling them to make informed choices. While I note that the guidance of the Article 29 Working Party is not binding on the Commission, it nevertheless is instructive in the understanding of transparency obligations and their relationship with the overarching principles enshrined in Article 5 GDPR. It is clear to me from the above that the purpose limitation principle has an important role to play, both in relation to the empowerment of the data subject, but also in relation to underpinning and supporting the objectives of the data protection framework as a whole under the GDPR.

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

5.40 The data controller must identify the categories of personal data that will be collected if they are to comply with the requirement to specify "purpose" in accordance with the purpose limitation principle. I am of the view that having access to the information required by Article 13(1)(c) GDPR in

conjunction with the category/categories of personal data being processed is essential if the data subject is to be empowered to hold the data controller accountable for compliance with the Article 5(1)(b) GDPR purpose limitation principle. The Article 29 Working Party reflects this approach in the Transparency Guidelines, by saying:

> "*Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles.*"[106]

5.41 For this reason, I expressed the view in the Preliminary Draft Decision that the information provided must set out: the purpose(s) of the specified processing operation/set of processing operations for which the (specified category/specified categories of) personal data are intended, and the legal basis being relied upon to support the processing operation/set of operations. In that information, there should be a clear link between the specified category/categories of data, the purpose(s) of the specified operation(s), and the legal basis being relied on to support the specified operation(s). In submissions on the Preliminary Draft Decision, the Complainant agreed with this position and that "[w]*ithout such linking, we would simply see generic lists of all data, all purposes and all legal bases under Article 6(1) GDPR without any indication of the relationships between them.*".[107]

5.42 However, Facebook disagreed with this analysis. To set out the position simply, Facebook argues that it is only obliged to provide specific information on (1) the purposes for the processing it carries out and (2) the legal bases upon which it relies. This amounts to simply setting out its own purposes (such as the examples in the paragraph above) and the legal bases upon which it relies for the collection and processing of personal data in order to fulfil those objectives. Its position is that two pieces of information are required and, in addition, argue that there is no requirement for the individual purposes to be linked with individual legal bases.

5.43 Facebook submits in contrast that such a "*third limb*" is not necessary. It submits that purpose and legal basis are "*conceptually, capable of being explained and understood without any reference to the practicalities of the processing operations*". It further submits that the provision of information on processing operations would in fact not aid transparency. In this regard, it also reiterates arguments already addressed above in relation to the alleged absence of a requirement under Article 13(1)(c) GDPR to specify processing operations.[108] Facebook specifically argues that it would be "*very difficult*

[106] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018.
[107] Complainant Submissions on Preliminary Draft Decision, page 20.
[108] *Ibid*, paragraph 8.3.

to achieve in ways that are "concise" and "intelligible", as required under Article 12(1) GDPR. This supposed requirement would therefore be intrinsically unlikely to assist data subjects or further the purposes behind the GDPR's transparency regime"[109]

5.44 As is evident from the assessments that follow, my view is that the Data Policy and related material sometimes, on the contrary, demonstrate an oversupply of very high level, generalised information at the expense of a more concise and meaningful delivery of the essential information necessary for the data subject to understand the processing being undertaken and to exercise his/her rights in a meaningful way. Furthermore, while Facebook has chosen to provide its transparency information by way of pieces of text, there are other options available, such as the possible incorporation of tables, which might enable Facebook to provide the information required in a clear and concise manner, particularly in the case of an information requirement comprising a number of linked elements. The importance of concision cannot be overstated nonetheless. Facebook is entitled to provide additional information to its user above and beyond that required by Article 13 and can provide whatever additional information it wishes. However, it must first comply with more specific obligations under the GDPR, and then secondly ensure that the additional information does not have the effect of creating information fatigue or otherwise diluting the effective delivery of the statutorily required information. That is simply what the GDPR requires.

5.45 In support of the argument that the Commission's interpretation of Article 13(1)(c) GDPR is incorrect, Facebook also refers to Article 14(1)(d) GDPR:

> "*14(1)(d) GDPR expressly requires a controller to provide information to the data subject on the categories of personal data (in circumstances where Article 14 applies) further reinforces this point - i.e. it is clear from the fact that the concept is referred to in Article 14(1)(d) GDPR, that the legislators made a deliberate choice not to include this concept in Article 13(1)(c) GDPR. Indeed, if the Commission's interpretation was correct there would have been no need for Article 14(1)(d) GDPR, as Article 14(1)(c) GDPR would in any event have to be approached on the basis that categories of data needed to be identified. As such, the Commission's approach appears to conflict with the statutory interpretation principle expressio unis est exclusio alterius*"[110]

5.46 In addressing this argument, it is important to underline the fundamental differences between Articles 13 and 14 GDPR. The first fundamental difference between Articles 13 and 14 GDPR is that Article 13 GDPR is expressly stated to apply in circumstances where "*personal data are collected from the data subject*". Article 14 GDPR, on the other hand, only applies in circumstances where personal data have been obtained from a source(s) other than the data subject. The second fundamental difference is that the information prescribed by Article 13 GDPR must be provided to the data subject

[109] *Ibid*, paragraph 8.2(F).
[110] *Ibid*, paragraph 8.4(C).

"*at the time when personal data are obtained*". The information prescribed by Article 14, however, can only be provided after the personal data has been collected.

5.47 These fundamental differences give rise to variations in the information required to be provided pursuant to Article 13 GDPR, on the one hand, and the information required to be provided pursuant to Article 14 GDPR, on the other. Firstly, Article 13(2)(e) GDPR requires the controller to inform the data subject as to "*whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.*" Article 14 GDPR, on the other hand, contains no such requirement. The rationale for this difference is clear. When this information is provided prior to the collection of personal data, the data subject is empowered to exercise control over their personal data. It avoids them being placed in a position where they provide personal data to the controller on a mistaken understanding as to either the necessity for its collection, or of the potential consequences of failure to provide it. The provision of such information would have no purpose if provided to the data subject after the personal data has been collected, hence its omission from Article 14 GDPR.

5.48 Secondly, Article 14(1)(d) GDPR requires that the data subject to be provided with information as to the "*categories of personal data concerned*" while Article 14(2)(f) GDPR requires the provision of information as to the source "*from which the personal data originate*". These requirements are notably absent from Article 13. The rationale for these omissions is clear by reference to the exemption to the obligation to provide information set out in Articles 13(4) and Article 14(5)(a) GDPR. These exemptions provide that the controller's obligation to provide the specified information "*shall not apply where and insofar as the data subject already has the information*". Therefore, both of these transparency provisions clearly envisage that they need not apply where the data subject has the information in question.

5.49 In some cases where personal data has been collected from the data subject, the data subject may already know the categories of personal data and the source of this information, because it is the data subject that has provided the personal data to the controller. Equally, however, some collection directly from the data subject is less obvious to the data subject for example where metadata or device data is collected from them. The data subject will, however, likely never have this knowledge if the data have been collected in the circumstances envisaged by Article 14 GDPR. It is therefore envisaged by both Articles 13 and 14 GDPR that in all circumstances, the data subject will have this information. In the case of Article 14 GDPR, the personal data has not been obtained by the data subject, and so Article 14 GDPR specifies that additional information should be provided. In the case of Article 13 GDPR, it may be the data subject who will have provided the data, and so the data subject may already know this information. In my view, this is the distinction between the provisions and the clear motivation of the legislator in including these categories of information in Article 14 GDPR alone.

5.50 Furthermore, it is unclear why a data subject would only be entitled to this information if the controller has acquired their personal data from another source. It is further difficult to understand how such a difference in treatment, between two categories of data subject, could be consistent with the GDPR, particularly where the difference in treatment concerns a core data subject right. If this were true, a data subject would only be entitled to this information if the personal data were obtained from a source other than themselves, but would not if it was obtained from them directly. This entirely arbitrary distinction is inconsistent with the clear aims of the GDPR to provide a series of universal rights to all data subjects, grounded on the universal right to data protection in Article 8 of the Charter. Therefore even if the interpretation advanced in the preceding paragraph were incorrect, Facebook's submissions would nonetheless not be supported by a purposive or systematic reading of the GDPR.

5.51 In any event, Facebook's submissions operate on the assumption that, as has been quoted above, Article 14(1)(d) GDPR would not be necessary if the Commission's interpretation of Article 13(1)(c) GDPR were applied *mutatis mutandis* to Article 14(1)(c) GDPR. This conflates the information the Commission's interpretation requires i.e. the "processing operations or sets of operations", and the information required by Article 14(1)(d) GDPR, i.e. "categories of personal data".

5.52 My view is Article 13(1)(c) GDPR therefore does require what has been described as the "third link" in this chain: the relevant information for the purposes of Article 13(1)(c) GDPR must be provided by reference to the processing operations themselves. This is supported both by a literal reading of the provision, having regard to the definition in Article 4(2) GDPR, and the systematic reading I have just set out above. This provision specifically refers to the purposes for which *the personal data* are intended. When the purposes and legal basis for processing are identified, they must be identified by reference to *the personal data* being processed or, at a minimum, the broad personal data processing operations to which they relate. The purposes and legal basis of processing personal data can only be understood by reference to the processing operations being undertaken. In order for information in this regard to be meaningful, and to provide data subjects with meaningful information as to whether they wish to exercise data subject rights, data subjects must be provided with this information. This goes to the essence of transparency in relation to the processing of personal data. In providing information on "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*" for the purposes of Article 13(1)(c) GDPR, the data controller must do so by reference to the personal data being processed or, at least, the broad personal data processing operations involved.

Information Provided by Facebook in Relation to Processing in Accordance With Article 6(1)(b) GDPR

5.53 The starting point in assessing this information provided by Facebook is the Data Policy. Facebook itself asserts that this is the document it uses to comply with the transparency obligations under Article 13(1)(b) GDPR. In the Data Policy, there is a section entitled "*What is our legal basis for processing data*?". The section dealing with contractual necessity is as follows:

> *"We collect, use and share the data that we have in the ways described above:*
>
> - *as necessary to fulfil our Facebook Terms of Service or Instagram Terms of Use"*

5.54 I note at this point that the Data Policy contains a hyperlink where users can "*Learn more about these legal bases and how they relate to the ways in which we process data*". This hyperlink is found at the end of the section partly quoted above, which lists processing carried out pursuant to each lawful basis under the GDPR. As I have set out in Section 2, this hyperlink directs Facebook users to an unnamed page that the Investigator terms the "Legal Basis Information Page". For clarity, I retain this definition. This page sets out that:

> "*For all people who have legal capacity to enter into an enforceable contract, we process data as necessary to perform our contracts with you (the Facebook Terms and Instagram Terms, together, 'the Terms'). We describe the contractual services for which this data processing is necessary in the "Our Services" section of the Terms, and in the additional informational resources accessible from the Terms. The core data uses necessary to provide our contractual services are:*
>
> - *To provide, personalize, and improve our Facebook Products;*
> - *To promote safety, integrity, and security;*
> - *To transfer, transmit, store, or process your data outside the EEA, including to within the United States and other countries;*
> - *To communicate with you, for example, on Product-related issues; and*
> - *To provide consistent and seamless experiences across the Facebook Company Products.*
>
> *These uses are explained in more detail in our Data Policy, under "How do we use this information?" and "How do we operate and transfer data as part of our global services?" and "How do the Facebook Companies work together?" We'll use the data we have to provide these services; if you choose not to provide certain data, the quality of your experience using the Facebook Products may be impacted.*"

5.55 It is clear from the above that Facebook users are invited to receive more information from other hyperlinked sources. In relation to the "Terms of Service" hyperlink, it directs users to the relatively lengthy Terms of Service which includes several other hyperlinks, including a hyperlink to the Data Policy. Users are also directed to the "Our Services" section of the Terms of Service, which sets out the following:

> "*Our mission is to give people the power to build community and bring the world closer together. To help advance this mission, we provide the Products and services described below to you:*

Provide a personalized experience for you:
Your experience on Facebook is unlike anyone else's: from the posts, stories, events, ads, and other content you see in News Feed or our video platform to the Pages you follow and other features you might use, such as Trending, Marketplace, and search. We use the data we have - for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products - to personalize your experience.

Connect you with people and organizations you care about:
We help you find and connect with people, groups, businesses, organizations, and others that matter to you across the Facebook Products you use. We use the data we have to make suggestions for you and others - for example, groups to join, events to attend, Pages to follow or send a message to, shows to watch, and people you may want to become friends with. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.

Empower you to express yourself and communicate about what matters to you:
There are many ways to express yourself on Facebook and to communicate with friends, family, and others about what matters to you - for example, sharing status updates, photos, videos, and stories across the Facebook Products you use, sending messages to a friend or several people, creating events or groups, or adding content to your profile. We also have developed, and continue to explore, new ways for people to use technology, such as augmented reality and 360 video to create and share more expressive and engaging content on Facebook.

Help you discover content, products, and services that may interest you:
We show you ads, offers, and other sponsored content to help you discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Facebook Products. Our partners pay us to show their content to you, and we design our services so that the sponsored content you see is as relevant and useful to you as everything else you see on our Products.

Combat harmful conduct and protect and support our community:
People will only build community on Facebook if they feel safe. We

employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example, offering help, removing content, blocking access to certain features, disabling an account, or contacting law enforcement. We share data with other Facebook Companies when we detect misuse or harmful conduct by someone using one of our Products.

Use and develop advanced technologies to provide safe and functional services for everyone:

We use and develop advanced technologies - such as artificial intelligence, machine learning systems, and augmented reality - so that people can use our Products safely regardless of physical ability or geographic location. For example, technology like this helps people who have visual impairments understand what or who is in photos or videos shared on Facebook or Instagram. We also build sophisticated network and communication technology to help more people connect to the internet in areas with limited access. And we develop automated systems to improve our ability to detect and remove abusive and dangerous activity that may harm our community and the integrity of our Products.

Research ways to make our services better:

We engage in research and collaborate with others to improve our Products. One way we do this is by analyzing the data we have and understanding how people use our Products. You can learn more about some of our research efforts.

Provide consistent and seamless experiences across the Facebook Company Products:

Our Products help you find and connect with people, groups, businesses, organizations, and others that are important to you. We design our systems so that your experience is consistent and seamless across the different Facebook Company Products that you use. For example, we use data about the people you engage with on Facebook to make it easier for you to connect with them on Instagram or Messenger, and we enable you to communicate with a business you follow on Facebook through Messenger.

Enable global access to our services:

To operate our global service, we need to store and distribute content and data in our data centers and systems around the world, including outside your country of residence. This infrastructure may be operated or controlled by Facebook, Inc., Facebook Ireland Limited, or its affiliates."

5.56 In addition, users are directed to the "How do we use this information" section of the Data Policy. It sets out the following:

"*We use the information we have (subject to choices you make) as described below and to provide and support the Facebook Products and related services described in the Facebook Terms and Instagram Terms. Here's how:*

Provide, personalize and improve our Products.
We use the information we have to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads) and make suggestions for you (such as groups or events you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide where you have given your explicit consent); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products. Learn more about how we use information about you to personalize your Facebook and Instagram experience, including features, content and recommendations in Facebook Products; you can also learn more about how we choose the ads that you see.

- *Information across Facebook Products and devices: We connect information about your activities on different Facebook Products and devices to provide a more tailored and consistent experience on all Facebook Products you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger. We can also make your experience more seamless, for example, by automatically filling in your registration information (such as your phone number) from one Facebook Product when you sign up for an account on a different Product.*

- *Location-related information: We use location-related information such*

as your current location, where you live, the places you like to go, and the businesses and people you're near-to provide, personalize and improve our Products, including ads, for you and others. Location related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Facebook Products (such as check-ins or events you attend).

- *Product research and development: We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.*

- *Face recognition: If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create are data with special protections under EU law. Learn more about how we use face recognition technology, or control our use of this technology in Facebook Settings. If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.*

- *Ads and other sponsored content: We use the information we have about you-including information about your interests, actions and connections-to select and personalize ads, offers and other sponsored content that we show you. Learn more about how we select and personalize ads, and your choices over the data we use to select ads and other sponsored content for you in the Facebook Settings and Instagram Settings.*

Provide measurement, analytics, and other business services.
We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services. Learn how we share information with these partners.

Promote safety, integrity and security.
We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security

> *on and off of Facebook Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to detect when someone needs help. To learn more, visit the Facebook Security Help Center and Instagram Security Tips.*
>
> ***Communicate with you.***
> *We use the information we have to send you marketing communications, communicate with you about our Products, and let you know about our policies and terms. We also use your information to respond to you when you contact us.*
>
> ***Research and innovate for social good.***
> *We use the information we have (including from research partners we collaborate with) to conduct and support research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. For example, we analyze information we have about migration patterns during crises to aid relief efforts. Learn more about our research programs."*

Facebook users are invited, by way of various hyperlinks, to receive further information on the matters set out above.

5.57 Facebook users are also invited, in the Legal Basis Information Page detailing processing based on Article 6(1)(b) GDPR, to consider the sections of the Data Policy entitled "How do we operate and transfer data as part of our global services" and How do the Facebook Companies work together?" The former states as follows:

> "*We share information globally, both internally within the Facebook Companies and externally with our partners and with those you connect and share with around the world in accordance with this policy. Information controlled by Facebook Ireland will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes as described in this policy. These data transfers are necessary to provide the services set forth in the Facebook Terms and Instagram Terms and to globally operate and provide our Products to you. We utilize standard contractual clauses approved by the European Commission and rely on the European Commission's adequacy decisions about certain countries as applicable for data transfers from the EEA to the United States and other countries*"

5.58 The latter states as follows:

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

> "*Facebook and Instagram share infrastructure, systems and technology with other Facebook Companies (which include WhatsApp and Oculus) to provide an innovative, relevant, consistent and safe experience across all Facebook Company Products you use. We also process information about you across the Facebook Companies for these purposes, as permitted by applicable law and in accordance with their terms and policies. For example, we process information from WhatsApp about accounts sending spam on its service so we can take appropriate action against those accounts on Facebook, Instagram or Messenger. We also work to understand how people use and interact with Facebook Company Products, such as understanding the number of unique users on different Facebook Company Products.*"

WHETHER FACEBOOK COMPLIES WITH ARTICLES 5(1)(A), 12(1) AND 13(1)(C) GDPR

5.59 As set out above, the information in the Legal Basis information Page and associated sections of the referenced Data Policy is provided by way of a summary in the Legal Basis Information Page, which directs users to various other documents and texts. The approach taken is somewhat disjointed in that the "summary" of the "core data uses" has been set out in expressly generalised terms, divorced from specific processing operations. If the user wishes to learn more, they must view the Terms of Service and also review the sections of the Data Policy to which they are directed. When all of the available information has been accessed, it becomes apparent that the texts provided are variations of each other, in that they re-iterate the goals and objectives of Facebook in carrying out data processing (for example, personalisation, communication, analytics, product improvement, etc.) rather than elaborating on this or providing information concerning processing operations. This approach lacks clarity and concision, and makes it difficult for the user to access meaningful information as to the processing operations that will be grounded on Article 6(1)(b) GDPR or on other legal bases. In my view, insufficient detail has been provided in relation to the processing operations carried out both in general and on the basis of Article 6(1)(b) GDPR specifically. Such an approach deprives the user of meaningful information and further risks causing significant confusion as to what legal basis will be relied upon to ground a specific processing operation.

5.60 In response to the Preliminary Draft Decision, the Complainant agreed with the approach taken on this issue, and emphasised that "*the most relevant change in Facebook's position*", in the Complainant's view is that the decision to rely on Article 6(1)(b) GDPR for the processing in question and not consent, following the GDPR taking legal effect, was contained in the last layer of information and not displayed prominently.[111]

5.61 In response to the Preliminary Draft Decision, which provisionally found that the information was provided in a disjointed manner and that the texts were variations of each other, Facebook submitted

[111] Complainant Submissions on Preliminary Draft Decision, page 19.

that it "*…maintains that the manner in which it has discharged its obligation under Article 13(1)(c) GDPR is entirely appropriate and compliant with the GDPR.*"[112] In particular, its position is that the documents have been structured so as to present the information in as simple a manner as possible. It also argues that the presence of information in separate hyperlinked pages that at times contains cross-over "*has been provided in a context where data subjects often wish to periodically seek out information of interest to them instead of digesting the entirety of these documents at once*".[113] It further defends the use of similar (but varied) text in the Data Policy to the Terms of Service on the grounds that they are distinct documents with distinct purposes, and that "[t]*he use of summary bullet points, instead of reproducing the relevant text from the Terms of Service in full makes the information more accessible to users regardless of their online or legal sophistication.*"[114]

5.62 I do not accept these arguments. First of all, while it remains the case that it is for Facebook to provide accessible information that is clear and concise for users regardless of their "sophistication", that does not detract from the core of the criticism that the disjointed information set out in generalised terms is "*divorced from specific processing operations*".[115] It is not that the presence of variations of the same information in several documents is of itself non-compliant, but rather that it is not compliant when it amounts, in practice, to statements about services and objectives that are not linked to specified processing operations and which do not provide meaningful information to the data subject on the core issues identified in Article 13 GDPR. The fact that this disjointed information is generalised and does not contain the required information (as has been set out when I addressed the correct interpretation of Article 13(1)(c) GDPR), renders the information as a whole unhelpful and ultimately inconsistent with Article 13 GDPR.

5.63 Put simply, it impossible to identify what processing operations will be carried out in order to fulfil the objectives that are repeated throughout the documents and the legal basis for such operations. In the absence of such information, the user is left to guess as to what processing is carried out on what data, on foot of the specified lawful bases, in order to fulfil these objectives. For the reasons set out above in relation to the correct interpretation of Article 13(1)(c) GDPR, this is insufficient information.

5.64 I note that some minimal information is provided in relation to the processing that will be carried out, notably in relation to location information and IP addresses. I note, however, that this is prefaced by "*such as*", and describes location-based information as "*things like…*" These are, in my view, clear examples of the open-ended language that is not conducive to the provision of information in a transparent manner. Moreover, it is unclear for what purpose this personal data is used, and indeed to what extent any such data might be (however minimally) processed to fulfil the objectives of the contractual relationship between Facebook and a user, and to what extent the processing of such data is based on another legal basis such as consent.

[112] *Ibid*, paragraph 8.10.
[113] *Ibid*.
[114] *Ibid*, paragraph 8.11(A).
[115] Paragraph 5.60 above.

5.65 Article 12(1) GDPR requires information to be provided in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*" The information that has been provided by Facebook is disjointed, and requires users to move in and out of various sections of the Data Policy and Terms of Service. I note that Facebook argues that "[c]*ritically, it is the Data Policy and the Legal Basis Information Page which are the means by which Facebook Ireland satisfies the requirements of Article 13(1)(c) GDPR (as explained above) – not the Terms of Service*".[116] As I have set out, however, I am not satisfied that the Data Policy and Legal Basis Information Page satisfy the requirements of Article 13(1)(c) GDPR either individually or cumulatively.

5.66 Facebook argues that it met the requirements of Article 12(1) GDPR and that:

> "*the GDPR allows considerable discretion for the controller as to the mode of compliance, taking into account its interests as well as those of data subjects its likely better understanding of both its services and its users, and; in particular allowing for a balancing of thoroughness with concision, intelligibility and accessibility. The obligation is not to provide information in a way that a particular supervisory authority (or anyone else) considers to be the best or preferred manner, but to do so in a way that meets an objective threshold standard.*"[117]

5.67 There is no doubt but that a controller has a certain amount of discretion as to the mode of compliance. Neither is there any question of a supervisory authority's "preferred manner" having any bearing on compliance with Article 12(1) GDPR, or any other provision. Rather it falls to the supervisory authority to assess compliance with the relevant provisions of the GDPR. In this case, there has been a failure to provide information in a concise manner in light of the failings associated with the disjointed and generalised nature of the documents in question. The information is neither concise nor transparent, and the language is neither clear nor plain, instead being expressed by reference to abstract objectives and purposes without any connection to specific categories of personal data or processing operations being undertaken.

5.68 Furthermore, it is concerning that, even if a user actively sought out the additional information that is available by way of the various links from the Terms of Service, the user would be presented with variations of information previously furnished rather than further and more detailed information that would enable the user to better understand the processing involved. By way of example, there is significant overlap between the information set out in the "How do we use this information" section of the Data Policy and the contents of the "Our Services" section of the Terms of Service. Similarly, the summary of "core uses" set out in the section of the Legal Basis Information Page that deals with Article

[116] Submissions on Draft Report, paragraph 7.1(A).
[117] *Ibid*, paragraph 9.3.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

6(1)(b) GDPR contains a sub-set of the information provided in the "Our Services" section of the Terms of Service. The way in which the information has been spread out on multiple subsections and has been drafted in similarly worded (and hyperlinked) text means that a user could easily overlook any new elements available within the linked text. It is not the case that a user would be presented with more detailed information once they go to the pages they are directed to; the information made available is similar in both substance and appearance to the information that is available both in the primary text and other hyperlinked texts. The submissions of Facebook on the Preliminary Draft Decision, as set out above, defend this practice. However, in my view, the varied sophistication of users is not a sufficient excuse to provide information that is, as I have set out, variations of the same thing rather than information that gradually becomes more detailed. This issue is compounded by the absence of information on processing operations themselves. Even the most sophisticated user would struggle to understand the purposes of the processing for which the personal data are intended as well as the legal basis for the processing in this context.

5.69 I emphasise that the Investigator, in preparing the Final Report, carried out a highly detailed and thorough analysis of the documents set out above and how they interrelate. While I have adopted a different approach, in not considering each "layer" in the abstract, I am equally convinced that the requisite information is neither present nor set out in a transparent manner. Moreover, I am of the view that, where this is the case on a cumulative reading of all of the documents (a matter on which I am in clear agreement with the Investigator), in this instance, nothing of substance turns on the question of whether an individualised assessment of each "layer" should be carried out.

5.70 I am of the view that the criticisms in the Complaint have merit to the extent that the information provided was not to the standard of clarity required by the GDPR. The way in which the relevant information has been presented requires the user to seek out the additional texts made available by way of the various hyperlinks. There is no single composite text or layered route available to the user such as would allow them to quickly and easily understand the full extent of processing operations that will take place as regards their personal data arising from their acceptance of the Terms of Service. Each additional layer presents the user with similar information to that already provided as well as some new information which is not easy to identify, as the language used is similar to the information that has been provided before. The user should not have to work so hard to access the prescribed information; nor should there be ambiguity as to whether all sources of information have been exhausted. This gives rise to real risks, such as those articulated by the Complainant, that there will be confusion as to what legal basis is being relied on for what processing operation(s). That is precisely what seems to have happened in the context of this Complaint, and is one of the main factual themes running through this entire Inquiry.

5.71 Information on the specific processing operations (necessarily including the data processed) that will be carried out for the purposes specified and by reference to the lawful bases specified (the latter two being currently, in my view, set out in a disjointed manner) should have been provided to the data subject. To the extent that this information was provided at all, it was not clearly linked with a specific

purpose or lawful basis, and was described in an ambiguous manner (such as in my analysis of the information on location-based data above).

5.72 The alleged "forced consent" and the dispute surrounding the processing operations being carried out, and the legal bases underpinning them, are reflective of a broader lack of clarity as regards the link between the purposes of processing, the lawful bases of processing and the processing operations involved. Article 13(1)(c) GDPR requires that this information be set out, and Article 12(1) GDPR requires that this same information be set out in a particular manner.

5.73 Finally, in its submission on the Preliminary Draft Decision, Facebook took issue with a proposed finding of an infringement of Article 5(1)(a) GDPR. In particular, Facebook argued that there cannot be an automatic infringement of Article 5(1)(a) GDPR simply because Articles 12(1) and 13(1)(c) GDPR have been infringed, or in the alternative that nothing further has occurred beyond the infringements to merit a finding of an infringement of Article 5(1)(a) GDPR.[118]

5.74 The Commission does not consider that an infringement of Article 5(1)(a) GDPR necessarily or automatically flows from findings of infringement under Articles 12 and/or 13 GDPR. Nevertheless, there is an important link between these provisions.

5.75 By way of elaboration, at the core of this Complaint lies an assumption on the Complainant's part that Facebook, which relied largely on consent as a matter of data protection law for the processing in question up to the coming into effect of the GDPR, was still relying on GDPR consent for the acceptance of the Terms of Service following the coming into effect of the GDPR. It has been submitted that this assumption was compounded by the engagement flow which presented users with a number of opportunities to consent, before the final "I agree".

5.76 While there is no particularised requirement under the GDPR to provide data subjects with information on an alteration of a legal basis, or to provide information in a particular part of any such engagement flow, the lack of clarity on such a fundamental issue underlines the inherent lack of transparency in the information provided to the data subject. Article 5(1)(a) links transparency to the overall fairness of the activities of a controller by requiring that personal data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*".[119] Having regard to the findings made above, it is appropriate for the Commission to make a finding that Facebook has also infringed Article 5(1)(a) GDPR in the circumstances of this case.

Finding 3:
In relation to processing for which Article 6(1)(b) GDPR is relied on, Articles 5(1)(a), 12(1) and 13(1)(c) have been infringed.

[118] Facebook Submissions on Preliminary Draft Decision, section 10.
[119] C Kuner et al eds, *The EU General Data Protection Regulation: A Commentary* (Oxford 2020), pages 314-315.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

6 SUMMARY OF FINDINGS

ISSUE	FINDING
Whether acceptance of the terms of service constitutes or must be consent for the purpose of GDPR	There is no obligation on Facebook to seek to rely solely on consent for the purposes of legitimising personal data processing where it is offering a contract to a user which some users might assess as one that primarily concerns the processing of personal data. Nor has Facebook purported to rely on consent under the GDPR.
Reliance on Article 6(1)(b) GDPR	I find the Complainant's case is not made out that the GDPR does not permit the reliance by Facebook on 6(1)(b) GDPR in the context of its offering of Terms of Service.
Whether Facebook 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	I find that Facebook has infringed Articles 5(1)(a), 12(1) and 13(1)(c) GDPR

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

7 DECISION ON CORRECTIVE POWERS

7.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my view to the effect that the Facebook has infringed Articles 5(1)(a), 12(1) and 13(1)(c) GDPR.

7.2 Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with Section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. For the reasons set out above and the reasons below, my view is that corrective measures should be imposed.

7.3 As I have set out, this is a Draft Decision that will be submitted by the Commission to other concerned supervisory authorities pursuant to Article 60 GDPR.

8 ORDER TO BRING PROCESSING INTO COMPLIANCE

8.1 Article 58(2) GDPR sets out the corrective powers which supervisory authorities may employ in respect of non-compliance by a controller or processor.

8.2 My view is that the corrective power provided for in Article 58(2)(d) GDPR, i.e. an order to bring processing into compliance, should be imposed. This order would require Facebook to bring the Data Policy and Terms of Service into compliance with Articles 5(1)(a), 12(1) and 13(1)(c) GDPR as regards information provided on data processed pursuant to Article 6(1)(b) GDPR, in accordance with the principles set out in this Draft Decision. Facebook argues that it is neither necessary nor proportionate to make this order.[120] For the reasons set out above and below, I have concluded that it is necessary and proportionate to do so.

8.3 It was proposed in the Preliminary Draft Decision that this order should be complied with within three months of the date of notification of any final decision. Facebook argued that this was not a reasonable period of time within which to make the necessary changes, as the changes would be resource-intensive and would require "*sufficient lead in time for preparing the relevant changes, conducting and taking account of user testing of the proposed changes, internal cross-functional engagement as well as of course engagement with the Commission, and localisation and translation of the information for countries in the European Region.*"[121]

8.4 Facebook is a large multinational organisation with significant financial, technological and human resources at its disposal. Moreover, the interim period, prior to any such rectification to the current lack of information being provided to data subjects, will involve a serious ongoing deprivation of their rights (as articulated in Section 9 below). Moreover, the Commission has provided specific

[120] Facebook Submissions on Preliminary Draft Decision, paragraph 11.
[121] *Ibid*, paragraph 12.4.

analysis to Facebook in relation to the correct interpretation of the provisions in question and the requisite information that is absent from the relevant user-facing documents. This specificity should negate any need for extensive engagement with the Commission during the period of implementation, and provides clarity for Facebook as to what objective its very significant resources should be directed towards in order to comply with this order. As such, I am not satisfied that it would be impossible or indeed disproportionate to make an order in these terms, having regard to the importance of the data subject rights involved, the specificity of the order and Facebook's resources.

8.5 I therefore order that the Terms of Service and Data Policy be brought into compliance within three months.

8.6 I consider that this order is necessary to ensure that full effect is given to Facebook's obligations under Articles 5(1)(a), 12(1), and 13(1)(c) GDPR in light of the infringements outlined above. The substance of this proposed order is the only way in which the defects pointed out in this Preliminary Draft Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that I am of the view that this power should be imposed. Facebook disagrees and states that it is already voluntarily attempting to alter the documents to express the views set out in the Preliminary Draft Decision, and would therefore like to continue using "*less onerous means*" to ensure compliance.[122]

8.7 However, having regard to the non-compliance in this Draft Decision, in my view, such an order is proportionate and is the minimum order required in order to guarantee that compliance will take place in the future. The fact that Facebook is already taking steps to bring its information into compliance would be nothing practically onerous about an order to carry out something that Facebook already intends to carry out. On that basis I see nothing in these arguments to suggest a lack of proportionality arises in relation to such an order.

9 ADMINISTRATIVE FINE

9.1 I note that Article 58(2)(i) GDPR permits me to consider the imposition of an administrative fine, pursuant to Article 83 GDPR, "in addition to, or instead of" the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in Section 115 of the 2018 Act, which permits the Commission to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2) GDPR. Article 83(1) GDPR, in turn, identifies that the administration of fines "*shall in each individual case be effective, proportionate and dissuasive*".

[122] *Ibid*, paragraphs 12.2 and 12.3.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

9.2 Further, when deciding whether or not to impose an administrative fine and the amount of any such fine, Article 83(2) GDPR requires me to give "*due regard*" to eleven criteria. Those criteria, together with my assessment of each, are set out below.

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

9.3 I note that Article 83(2)(a) GDPR requires consideration of the identified criterion by reference to "the infringement" as well as "the processing concerned". Considering first the meaning of "infringement", it is clear from Articles 83(3)-(5) GDPR, that "infringement" means an infringement of a provision of the GDPR. In the context of this Inquiry, I propose findings that reflect my view that Facebook infringed Articles 5(1)(a), 12(1) and 13(1)(c) GDPR . Thus, "the infringement", for the purpose of my assessment of the Article 83(2) GDPR criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Articles 5(1)(a), 12(1) and 13(1)(c) GDPR. While each is an individual "infringement" of the relevant provision, they all concern transparency and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) GDPR assessment criteria. Accordingly, and for ease of review, I will assess all three infringements simultaneously, by reference to the collective term "Infringements", unless otherwise indicated to the contrary.

9.4 The phrase "the processing concerned" should be understood as meaning all of the processing operations that Facebook carries out on the personal data under its controllership for which is relies on Article 6(1)(b) GDPR. The within Inquiry was based on an assessment of the extent to which Facebook complies with its transparency obligations in the context of a specific Complaint. The Inquiry examined, *inter alia* the extent of the information Facebook provided to the Complainant about processing carried out pursuant to Article 6(1)(b) GDPR. Given the generality of the Complaint and therefore the Inquiry, the precise parameters of this processing were not directly relevant to the factual analysis carried out. The phrase "the processing concerned" therefore refers simply to the processing addressed in the Preliminary Draft Decision i.e. the permissibility in principle of processing personal data for behavioural advertising.

9.5 From this starting point, I will now assess the Article 83(2)(a) criterion in light of the particular circumstances of the Inquiry. I note, in this regard, that Article 83(2)(a) comprises the nature, gravity and duration of the infringement; the nature, scope or purpose of the processing concerned; the number of data subjects affected; and the level of damaged suffered by them; as follows:

Nature, gravity and duration of the infringement

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

9.6 In terms of the nature of the Infringements, the proposed findings concern infringements of the data subject rights. As set out in the analysis of Article 13(1)(c) GDPR above, my view is that the right concerned – the right to information – is a cornerstone of the rights of the data subject. Indeed, the provision of the information concerned goes to the very heart of the fundamental right of the individual to protection of personal data which stems from the free will and autonomy of the individual to share their personal data in a voluntary situation such as this. If the required information has not been provided, the data subject has been deprived of the ability to make a fully informed decision as to whether they wish to use a service that involves the processing of their personal data and engages their associated rights. Furthermore, the extent to which a data controller has complied with its transparency obligations has a direct impact on the effectiveness of the other data subject rights. If data subjects have not been provided with the prescribed information, they may be deprived of the knowledge they need in order to consider exercising one of the other data subject rights.

9.7 I further note, in this regard, that Articles 83(4) and (5) GDPR are directed to the maximum fine that may be imposed in a particular case. The maximum fine prescribed by Article 83(5) GDPR is twice that prescribed by Article 83(4) GDPR. The infringements covered by Article 83(5) GDPR include infringements of the data subject's rights pursuant to Article 12 to 22 GDPR and infringements of the principles in Article 5 GDPR. It is therefore clear that the legislator considered the data subject rights and the Article 5 GDPR principles to be particularly significant in the context of the data protection framework as a whole.

9.8 Facebook has argued that the nature of the infringements amount to a good faith difference of opinion, and present a new and subjective interpretation of the GDPR.[123] As part of my assessment of the Article 83(2)(c) GDPR criterion, which requires consideration of "any action taken by the controller or processor to mitigate the damage suffered by data subjects", I note that it would be unfair to criticize Facebook for failing to take action to mitigate any damage suffered in circumstances where its position was that no infringement had occurred and, accordingly, no damage had been suffered by data subjects. This does not, however, do anything to alter the infringement's objectively serious character.

9.9 In terms of the gravity of the Infringements, my findings are such that Facebook has not provided the required information in the required manner under Article 13(1)(c) GDPR and has also infringed Articles 12(1) and 5(1)(a) GDPR. This, in my view, represents a significant level of non-compliance, taking into account the importance of the right to information, the consequent impact on the data subjects concerned and the number of data subjects potentially affected (each of which is considered further below).

[123] Facebook Submissions on Preliminary Draft Decision, paragraph 13.2.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

9.10 Facebook argues that the infringements are on the lower end of the scale in their nature and gravity because the Commission's interpretation amounts to new and subjective views being imposed on it.[124] I do not accept that these views are new or subjective. I set out at Section 5 in great detail the extent to which this level of compliance is expected by the transparency guidelines, which are a publicly available document. The clear inconsistencies between the transparency guidelines and the manner in which Facebook attempted to comply with its obligations makes clear that the Commission's interpretation is neither new nor subjective. The Commission is carrying out its functions under the GDPR, by interpreting and applying the relevant provisions of the GDPR to the Complaint before it. Facebook also argues that no evidence has been presented of the impact on data subjects from a lack of transparency.[125] On the contrary, this entire Complaint arises from a failure to provide sufficiently transparent information such that the Complainant could understand the agreement to the Terms of Service was not consent in the sense meant in the GDPR. Moreover, I have already set out in Section 5 the risks to data subjects in being unable to effectively exercise their rights by being unable to discern what specific data processing is being done on what legal basis and for what objective. This is more than sufficient to show the negative impact that this has had on data subjects and specifically on the Complainant. Given that this concerns a significant impact in the manner set out in this Draft Decision, I cannot accept the suggestion from Facebook that the proposed administrative fine be replaced with a reprimand.[126]

9.11 In terms of the duration of the Infringements, this complaint-based Inquiry relates in part to a lack of information provided to the Complainant as regards the lawful basis relied on and the connection between Article 6(1)(b) GDPR and specific processing operations or sets of operations. The Complaint therefore relates to the transparency of the relevant documents at the time the Complaint was lodged. In that sense, this Inquiry relates to specific alleged infringements at a specific point in time, because that is what the Complaint concerns. In imposing corrective powers however, the GDPR requires that the broader impact of infringements be considered (as I will set out below in relation to each individual criterion). To that extent, it is necessary at times to move from the specific to the general.

9.12 I note at this juncture that Facebook has taken issue with various alleged inconsistencies between the approach to factors considered in administrative fines in the Preliminary Draft Decision and in other decisions made by the Commission under the GDPR to date.[127] The Commission does not agree that there is any inconsistency in the manner in which it has assessed the Article 83(2) GDPR criteria. The Commission is not required to apply the same approach across all inquiries, regardless of the differences between such 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,

[124] *Ibid*.
[125] *Ibid.*
[126] *Ibid.*
[127] *Ibid*, paragraph 14.2.

particularly as concerns the scale of the processing at issue. Unlike the position with the smaller-scale domestic inquiries to which Facebook refers, inquiries into larger internet platforms generally concern data controllers or processors with multi-national operations and significant resources available to them, including large, in-house, compliance teams.

9.13 Moreover, such entitles are further likely to be engaged in business activities that are uniquely dependent on the large-scale processing of personal data. The Commission's view is that the size and scale of such entities, the level of dependency on data processing and the extensive resources that are available to them necessitate a different approach to the absence of previous relevant infringements. That approach has been reflected in the decisions that differ in their considerations of particular factors from this one. In the circumstances, the Commission does not accept that there has been an inconsistency in the Commission's approach to determining the quantum of any fine.

Taking into account the nature, scope or purpose of the processing concerned

9.14 The personal data processing carried out by Facebook pursuant to Article 6(1)(b) GDPR is extensive. Facebook processes a variety of data in order to serve users personalised advertisements, tailor their "News Feed", and to provide feedback to advertising partners on the popularity of particular advertisements. The processing is central to and essential to the business model offered, and, for this reason, the provision of compliant information in relation to that processing becomes even more important. This, indeed, may include location and IP address data.

The number of data subjects affected

9.15 Facebook has confirmed that, as of the date of the Complaint, it had approximately 235 monthly active users and, as of May 2021, it had approximately 265 million monthly active users in the European Economic Area.[128]

9.16 Eurostat, the statistical office of the European Union confirms that, as of 1 January 2020, the population of the ""EU 27" was approximately 488 million, the population of the UK was approximately 67 million, the population of Norway was approximately 5 million, and the populations of Iceland and Liechtenstein were approximately 364,000 and 39,000 respectively.[129]

9.17 By reference to these figures, the total population of the EEA (including the UK) by reference to the latest available figures is approximately 520 million. While it is not possible, or indeed necessary, for me to identify the precise number of users affected by the Infringements, it is useful to have some point of reference in order to consider the extent of EEA data subjects that are potentially affected by the Infringements. The figures available for Facebook equates to

[128] *Ibid,* paragraph 4.11.

[129] https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001&plugin=1.

approximately 50-55% of the population of the EEA (including the UK), by reference to the Eurostat figures above.

The level of damage suffered by them

9.18 I note 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 …*"

9.19 As set out above, my findings are such that users have not been provided with the information in relation to processing pursuant to Article 6(1)(b) GDPR that they are entitled to receive. This represents, in my view, quite a significant information deficit and one which, by any assessment of matters, can equate to a significant inability to exercise control over personal data. I have also pointed out the centrality of the processing to Facebook's business model. This makes it all the more important that information on this processing be provided in a transparent manner, and makes the implications of it not being provided in such a manner all the more significant.

9.20 I further note that the failure to provide all of the prescribed information undermines the effectiveness of the data subject rights and, consequently, infringes the rights and freedoms of the data subjects concerned. A core element of transparency is empowering data subjects to make informed decisions about engaging with activities that cause their personal data to be processed, and making informed decisions about whether to exercise particular rights, and whether they can. This right is undermined by a lack of transparency on the part of a data controller.

9.21 Facebook argues that the above amounts to mere speculation.[130] I have already set out in detail in this Draft Decision the risks to data subject rights involved in the denial of transparency, and indeed provided the concrete example of the breach of the Complainant's rights to transparency about the use of her personal data. This is more than sufficient to show that rights have been damaged in a significant manner, given the lack of an opportunity to exercise data subject rights while being fully informed.

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

[130] Facebook Submissions on Preliminary Draft Decision, paragraph 4.13.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

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

> "*In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*"[131]

9.23 The Administrative Fines Guidelines go on to distinguish between circumstances that are indicative of 'intentional breaches' and those that are indicative of breaches occasioned by unintentional, or negligent, conduct. In this regard, the Guidelines cite "*failure to read and abide by existing policies*" and "*human error*" as being examples of conduct that may be indicative of negligence.

9.24 The Complainant has clearly asserted that the alleged infringements on Facebook's part were intentional acts. Moreover, the character of the infringement is that it was a decision made knowingly to present information in a particular way. Facebook is however entitled to a hold differing position in relation to the interpretation of particular provisions of the GDPR. While Facebook may have believed that it was in compliance with the GDPR, it is my view that the infringements arose out of a deliberate decision. It is important that Facebook provides clarity about the precise extent of the processing operations carried out pursuant to Article 6(1)(b) GDPR and that it adheres strictly to its transparency obligations when choosing the lawful bases on which they rely.

9.25 Facebook cites the above passage from the Fining Guidelines to support its position that "intention" refers to a deliberate breach of the GDPR rather than a deliberate act.[132] I note in this regard that the Fining Guidelines refer to two requirements, "knowledge" and "wilfulness". This suggests a controller must infringe the GDPR both in full knowledge of the infringement's characteristics and also in a deliberate manner. Having considered the nature of the infringements further in the context of the Fining Guidelines, I accept Facebook's submissions that any intentional breach must be an intentional and knowing breach of a provision of the GDPR. There is no evidence that this has taken place.

[131] Article 29 Working Party "Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679", page 11.
[132] Facebook Submissions on Preliminary Draft Decision, paragraph 4.14.

9.26 Facebook also argues that even if the position on the definition of intent is accepted, what occurred was not a deliberate act but an omission.[133] In light of my finding in the above paragraph it is unnecessary to consider this submission.

9.27 I am therefore satisfied that the failure to provide the requisite information was negligent in character. Facebook is under a clear legal duty to correctly apply the law and it has not done so. This amounts to a breach of the duty imposed by the provisions of the GDPR, and is on that basis a negligent infringement.

ARTICLE 83(2)(C): ANY ACTION TAKEN TO MITIGATE THE DAMAGE TO DATA SUBJECTS

9.28 Facebook's position is that its approach to transparency, in the context in which infringements have been found, complies fully with the GDPR. Notwithstanding my proposed disagreement with this position, I accept that it represents a genuinely held belief on Facebook's part. This does not alter the fact that infringements have occurred. On that basis, there has been no effort to mitigate the damage to data subjects, given Facebook's position was that no damage was taking place.

9.29 Facebook argues that this analysis is flawed because it takes no account of the effort made to comply with the GDPR. There is no reason why, on the basis of Transparency Guidelines, Facebook could not have taken steps to ensure compliance and thereby mitigate damage. I am not satisfied that there is any reason why day-to-day compliance related activities in a large multinational organisation, which is an important legal duty and commonplace business activity, could be considered a mitigating factor. Taking steps to attempt to comply with legal obligations is a duty, and has no mitigating impact on a sanction for a breach of those obligations. This is distinct from any act that might be taken to mitigate specific damage to data subjects. I am not of course treating this factor as aggravating given that, beyond simply complying with the GDPR, there are no obvious mitigating steps that could have been taken. It is on this basis that I treat this factor as neither mitigating nor aggravating.

9.30 I do, however, take account of and acknowledge Facebook's willingness to engage in steps to bring its processing into compliance on a voluntary basis pending the conclusion of this Inquiry. I consider this to be a mitigating factor.

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

9.31 The Fining Guidelines set out that:

[133] *Ibid*.

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

9.32 In relation to Facebook's responsibility from a technical and organisational perspective, Facebook has argued that, given it did not deliberately and knowingly break the law. It could not be said to have responsibility "*at the highest level*".[134] While I accept this this argument and have revised my provisional view. I nonetheless consider that Facebook's responsibility is certainly at a high level.

9.33 In this regard, I once again emphasise that the position as implemented represented a genuinely held belief, and the modes of implementation of compliance utilised by Facebook in this regard constituted a genuine effort to implement compliance based on this genuinely held belief. This genuine effort, however, has ultimately fallen short in terms of compliance in significant respects. I have found that it concerns serious data processing, and that it was deliberate act, in spite of the genuinely help belief that the modes of implementation were compliant. The degree of responsibility on Facebook's part is therefore, in my view, responsibility of a high level.

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

9.34 There have been no relevant previous infringements by Facebook of the GDPR in this regard on which findings have been made. Facebook once again compares the lack of mitigation in this regard to a decision of the Commission on a domestic matter.[135] I have already set out my views on these arguments above. Further, the Article 83(2) GDPR criteria are matters that I must consider when deciding whether to impose an administrative fine and, if so, the amount of that fine. The Article 83(2) GDPR criteria are not binary in nature, such that, when assessed in the context of the circumstances of infringement, they must be found to be either a mitigating or an aggravating factor.

9.35 Accordingly, it does not follow that the absence of a history of infringement must be taken into account as a mitigating factor. This is particularly the case where the GDPR has only been in force for a relatively short period of time. On this basis, my view is that this is neither a mitigating factor nor an aggravating one for the purpose of this assessment.

[134] *Ibid*, paragraph 14.16.
[135] *Ibid*, paragraphs 4.17-4.18.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

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

9.36 The Fining Guidelines state that:

> "*… it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspection.*"

9.37 Facebook argues that cooperation in this matter should be treated as a mitigating factor, and again cites a decision of the Commission.[136] I once again refer to my analysis on that issue above. Furthermore, I cannot accept that such activity, in the ordinary course of adhering to legal duties to cooperate and engage with a regulator, could be found to be a mitigating factor in a sanction. If this were the case, all controllers would get the benefit of such a mitigating factor aside from those that did not actively behave in an uncooperative manner. This position reflects the erroneous treatment of the Article 83(2) GDPR factors as binary choices between mitigation and aggravation to which I have already referred. I note once again that Facebook is seeking to voluntarily comply, and note that I have already taken this into account above as a mitigating factor

9.38 For these reasons, while Facebook has cooperated fully with the Commission at all stages of the Inquiry, it is required to do so by law. Furthermore, I note that the cooperation that would be relevant to the assessment of this criterion is cooperation "*in order to remedy the infringement and mitigate the possible adverse effects of the infringement*". In the circumstances, and in light of my views set out above, nothing arises for assessment by reference to this criterion.

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

9.39 The lack of transparency concerned broad categories of personal data relating to users who sign up to the service. I have set out several times in this Draft Decision that the assessment of data processing in this Inquiry was, by its nature, rather generalised. Indeed, the lack of transparency on Facebook's part has itself contributed to a lack of clarity on precisely what categories of personal data are involved. I therefore agree with Facebook's submission that this is not an aggravating factor,[137] and I also do not regard it as a mitigating one.

[136] *Ibid*, paragraph 14.19.
[137] *Ibid*, paragraph 14.20.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

ARTICLE 83(2)(H): THE MANNER IN WHICH THE INFRINGEMENT BECAME KNOWN TO THE SUPERVISORY AUTHORITY, IN PARTICULAR WHETHER, AND IF SO TO WHAT EXTENT, THE CONTROLLER OR PROCESSOR NOTIFIED THE INFRINGEMENT

9.40 The subject matter became known to the Commission due to an Inquiry conducted on foot of the Complaint. The subject matter did not give rise to any requirement of notification, and I have already acknowledged several times that the controller's genuinely held belief is that no infringement is/was occurring.

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

9.41 This criterion is not applicable.

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

9.42 This criterion is not applicable.

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

9.43 In the Preliminary Draft Decision I considered the following factors:

- Facebook does not charge for its service.
- The subject matter of the infringement relates directly to the provision of information in relation to what is, by Facebook's own admission, its core business model i.e. personalised advertising provided pursuant to a contract with users.
- The question is therefore whether a more transparent approach to processing operations carried out on foot of that contract would represent a risk to Facebook's business model. In my l view it would, if existing or prospective users were dissuaded from using the service by clearer explanations of the processing operations carried out, and their purposes.

- In my view the above risk is sufficiently high to justify the conclusion that this lack of transparency has the potential to have resulted in financial benefits for Facebook.

9.44 Facebook however argues that this does not at all propose a financial risk, and argues that no evidence of same has been presented.[138] Neither I nor Facebook can know, until the contingent event has happened, which one of us is correct in our belief as to the likely impact, on the continued growth of the user base. Given that any general consideration of this is ultimately involves an element of speculation on both Facebook's and the Commission's part, I consider that this factor is neither aggravating nor mitigating.

WHETHER TO IMPOSE AN ADMINISTRATIVE FINE

9.45 I am proposing to impose an administrative fine in circumstances where:

- The infringements are serious in nature. The lack of transparency goes to the heart of data subject rights and risks undermining their effectiveness by not providing transparent information in that regard. While the infringements considered here relate to one lawful basis, it nonetheless concerns vast swathes of personal data impacting millions of data subjects. When such factors are considered, it is clear that the infringements are serious in their gravity.

- Over 50% of the population of the EEA seems to be impacted by the infringements. This is a very large figure.

- I note in particular the impact a lack of transparency has on a data subject's ability to be fully informed about their data protection rights, or indeed about whether in their view they should exercise those rights.

- I have already found that the infringement was negligent. While I am not calling into question Facebook's right to come to a genuine view on this matter, I am taking into account the failure of an organisation of this size to provide sufficiently transparent materials in relation to the core of its business model.

[138] *Ibid*, paragraph 14.21.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

- I note that Facebook's Data Policy and Terms of Service have been amended, and because this is an Inquiry into a particular complaint the documents being considered are no longer contemporary. Therefore, I am not attaching significant weight to the question of the duration of the infringement, in circumstances where more recent versions of the relevant documents are outside the scope of the Inquiry.

- The mitigating factor of Facebook's decision to begin preparation for voluntary compliance on the basis of the views set out in the Preliminary Draft Decision

.

9.46 Facebook argues that the infringements set out above are "*co-extensive*" and amount to the same infringement.[139] It is incorrect to state that these amount to different labels for the same infringement. One amounts to a failure to provide information that is required by the law. The other amounts to a failure to provide the information required by the law (only some of which has been provided) in the manner the law requires. The information that is and is not provided both relate to data processing on foot of one provision of the GDPR. That does not in and of itself render them the same infringement. A failure to provide certain information and a failure to set out other information in a particular manner are self-evidently different infringements in their character.

9.47 Based on the analysis I have set out above, the nature, gravity and duration of the infringements and the potential number of data subjects affected, I propose to impose the following administrative fines:

- In respect of the failure to provide sufficient information in relation to the processing operations carried out on foot of Article 6(1)(b) GDPR, thereby infringing Articles 5(1)(a) and 13(1)(c) GDPR, I propose a fine of between €18 million and €22 million.

- In respect of the failure to provide the information that was provided on the processing operations carried out in foot of Article 6(1)(b) GDPR, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, thereby infringing Articles 5(1)(a) and 12(1) GDPR, I propose a fine of between €10 million and €14 million.

[139] *Ibid*, paragraph 15.1.

9.48 In having determined the quantum of the fines proposed above, I have taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be "*effective, proportionate and dissuasive*" in each individual case. My view is that, in order for any fine to be "effective", it must reflect the circumstances of the individual case. As already discussed above, the Infringements are serious, both in terms of the extremely large number of data subjects potentially affected, the categories of personal data involved, and the consequences that flow from the failure to comply with the transparency requirements for users.

9.49 In order for a fine to be "dissuasive", it must dissuade both the controller/processor concerned as well as other controllers/processors carrying out similar processing operations from repeating the conduct concerned.

9.50 As regards the requirement for any fine to be "proportionate", this requires me to adjust the quantum of any proposed fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fines proposed above do not exceed what is necessary to enforce compliance with the GDPR, taking into account the size of Facebook's user base, the impact of the Infringements on the effectiveness of the data subject rights enshrined in Chapter III of the GDPR and the importance of those rights in the context of the GDPR as a whole.

9.51 Accordingly, I am satisfied that the fines proposed above would, if imposed on Facebook, be effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

9.52 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.

10 OTHER RELEVANT FACTORS

ARTICLE 83(3) GDPR

10.1 Article 83(3) GDPR provides that:

"*If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*"

10.2 As outlined previously, Facebook's infringements of Articles 5(1)(a), 13(1)(c), and 12(1) GDPR all relate to the same processing operations concerning its processing carried out in accordance with Article 6(1)(b) GDPR. Therefore, the total amount of the administrative fine must not exceed the amount specified for the gravest infringement. The gravest infringement identified is the failure to provide the information mandated by Articles 13(1)(c) and 5(1)(a) GDPR.

10.3 Subsequent to the finalisation of the Preliminary Draft Decision, the EDPB adopted a binding decision ("**the EDPB Decision**")[140] relating to IN 18-12-2, an inquiry conducted by the Commission into WhatsApp Ireland Limited's compliance with Articles 12, 13 and 14 GDPR. The EDPB Decision arose out of a dispute resolution procedure pursuant to Article 65 GDPR, and was adopted by the Commission in conjunction with the Commission's final decision on 2 September 2021.

10.4 The EDPB Decision applies an interpretation of Article 83(3) GDPR that differs from the interpretation I set out in the Preliminary Draft Decision. In light of the Commission's obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR, it is necessary for me to follow the EDPB's interpretation of Article 83(3) GDPR in future inquiries given that it is a matter of general interpretation that is not specific to the facts of the case in which it arose.

10.5 The relevant passage of the EDPB decision is as follows:

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

140 https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.

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

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

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

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

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

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

324. With regard to the meaning of Article 83(3) GDPR the EDPB, bearing in mind the views expressed by the CSAs, notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording "amount specified for the gravest infringement" refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 state that the "occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.

325. The wording "total amount" also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording "total amount" in this regard already implies that other infringements have to be taken into account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.

326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed.

> *Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.*
>
> *327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness."*

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

10.7 In this Inquiry, the gravest infringement is that of the failure to provide information on data processing carried out pursuant to Article 6(1)(b) GDPR, in contravention of Articles 5(1)(a) and 13(1)(c) GDPR. The associated maximum possible fine for this infringement under Article 83(5) GDPR is 4% of the turnover of Facebook Inc. It is further to be noted that the EDPB's Decision, from which I quoted above, also directed the Commission to take account of the undertaking's turnover in the calculation of the fine amounts and I therefore factor that turnover figure below into my calculations of the individual infringement fining ranges. When the proposed ranges for the individual infringements are added together, a fining range of between €28 million and €36 million arises. This is below 4% of the turnover of Facebook Inc. as considered below.

10.8 As the EDPB Decision was adopted subsequent to Facebook having made submissions on the Preliminary Draft Decision, I afforded Facebook an opportunity to make submissions on this specific matter: that is, the EDPB's interpretation of Article 83(3) GDPR.

10.9 As a preliminary matter Facebook has objected to the manner in which it has been asked to make submissions on this interpretation, and in particular that it was provided with an extract copy of a working draft rather than an entire copy of the working draft of the Draft Decision. This, in its view, results in a requirement to make submissions "*in the abstract*" without having sight of the reasoning for the alteration of the fining range.[141]

[141] *Ibid*, paragraph 2.1.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

10.10 As is set out in this Draft Decision, Facebook has already been afforded an opportunity to make comprehensive submissions on the Preliminary Draft Decision that addressed every factor proposed by the Commission for consideration in determining, if any, the appropriate fine. It was not the intention of the Commission, in this regard, to seek additional submissions from Facebook on the reasoning for a particular fining range, those submissions having already been made in detail. The purpose of requesting new submissions, on this point, was to enable Facebook to exercise a right to be heard on the application of the interpretation of Article 83(3) GDPR in the EDPB Decision. On this basis, I do not accept that Facebook has been deprived of the opportunity to "*meaningfully exercise right to be heard*".[142]

10.11 On the substance, Facebook has argued that the above interpretation and application of Article 83(3) GDPR is incorrect and/or should not be applied because: the EDPB decision is incorrect as a matter of law and is, in any event, not binding on the Commission; even if the decision were binding on the Commission, it does not require that the Commission impose administrative fines in the manner proposed; the Commission has not had regard to the criteria of effectiveness, proportionality and dissuasiveness in Article 83(1) GDPR when determining the total cumulative proposed fine; and no decision on the correct interpretation of Article 83(3) GDPR should be made prior to the determination of a pending application by WhatsApp Ireland, pursuant to Article 263 TFEU, before the General Court of the Court of Justice of the European Union, to annul the EDPB Decision ("the **Annulment Proceedings**").[143]

10.12 Facebook's first substantive submission on this matter is that the EDPB Decision is not binding on the Commission. A number of legal arguments are made in this regard, including that binding decisions of the EDPB only apply to specific individual cases (as set out in article 65(1) GDPR)[144] and that only the CJEU can issue binding decisions on matters of EU law.[145] For the avoidance of doubt, the Commission has not expressed the view, nor does it hold the view, that the EDPB Decision is legally binding on it in this Inquiry and/or generally. The Commission is nonetheless, in this regard, bound by a number of provisions of the GDPR and the real question that arises in this context is the extent to which the Commission should have regard to the EDPB's approach.

10.13 The Commission is bound by Article 60(1) GDPR, which states in the imperative that "*the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus*" [emphasis added]. The Commission is similarly required to cooperate with other supervisory authorities, pursuant to

[142] *Ibid*.
[143] Facebook Submissions 9 September 2021, paragraph 1.2.
[144] *Ibid*, paragraph 3.4.
[145] *Ibid*, paragraph 3.6.

Article 63 GDPR. Facebook has argued that these obligations relate only to specific cases where a dispute has arisen.[146] Moreover, it submits that the EDPB's function in ensuring correct application of the GDPR is provided for instead in Article 70(1) GDPR, such as through issuing opinions and guidelines.[147]

10.14 It is not the position of the Commission that the EDPB in and of itself has the power to issue decisions of general application that bind supervisory authorities. The issue is not the powers or functions of the EDPB, but rather the legal responsibility of the Commission to the concerned supervisory authorities, who in themselves happen to be constituent members of the EDPB. In this regard, assistance is provided in the interpretation of the Commission's duties under Article 60(1) GDPR by Recital 123, which states that "…*supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union*…". The Commission's view is that the duty to cooperate and ensure consistency that is placed on it by the GDPR would be rendered ineffective were it not to ensure, to the best of its ability, such interpretations were applied consistently.

10.15 The alternative scenario, as proposed by Facebook, would result in entrenched interpretations being consistently advanced by individual supervisory authorities. The consequence would be inevitable dispute resolution procedures under Article 65 GDPR, and the issuing of a binding decision once again applying an alternative interpretation to the specific facts at hand that had already been comprehensively addressed in a previous dispute resolution procedure. Such a scenario would deprive the duties to cooperate and act consistently of almost any meaning. In the Commission's view, such an interpretation would therefore be contrary to the principle of *effet utile*. This is, as has been set out, a distinct issue from the legal powers or functions of the EDPB itself.

10.16 Facebook has argued that the EDPB Decision "*did not direct the* [Commission] *to impose separate fines in respect of each infringement and to then add those fines together*", but rather that the final amount should be considered in accordance with the requirements that the fine be effective, proportionate and dissuasive pursuant to Article 83(1) GDPR. It submits that overlap between the infringements should be taken into account, in this regard.[148] It goes on to argue that as there is *"…significant – if not complete – overlap between the infringements"*[149] and that the fines relate to *"…what is essentially the same set of facts and alleged infringement…"*, the fine is contrary to the EU law principles of proportionality, *ne bis in idem* and concurrence of laws.[150]

[146] *Ibid*, paragraph 3.3.
[147] *Ibid*, paragraph 3.5.
[148] *Ibid*, paragraph 4.2.
[149] *Ibid*, paragraph 4.4.
[150] *Ibid*, paragraph 4.3.

10.17 Facebook develops this aspect of its argument in a later section of its submission, by suggesting that "*it appears…that the* [Commission] *does not propose to engage in any meaningful assessment of whether the total fine* [meets the Article 83(1) GDPR criteria]".[151] Facebook argues that because the Commission viewed the fine proposed in the Preliminary Draft Decision as effective, proportionate and dissuasive, a fine that is between €8 million and €12 million higher must go beyond that standard.[152] Facebook also argues that its ability to make submissions in relation to this new proposed fine is "*restricted*" due to it not being given sight of the entire working draft but simply of the working draft relevant to the application of the EDPB's interpretation of Article 83(3) GDPR.[153]

10.18 In relation to the requirements of Article 83(1) GDPR, which includes the EU law principle of proportionality relied on by Facebook, the Commission refutes any suggestion that it has not had regard to this provision in proposing a final fine. The concluding six paragraphs of Section 9 of this Draft Decision set out, in detail, the Commission's reasoning as to why the proposed fine is effective, proportionate, and dissuasive. Moreover, as has been set out, Facebook has provided extensive submissions on the Preliminary Draft Decision as to its views on what an effective, dissuasive and proportionate sanction would be. I therefore reject any suggestion that there was "*a failure to adequately consider whether, taken as a whole, the proposed fines in respect of all the infringements are effective, proportionate and dissuasive*". [154]

10.19 Facebook has already provided submissions on the Preliminary Draft Decision, which clearly set out its view on the approach to fines in this matter, without prejudice to its view that no infringement of the GDPR has taken place. The purpose of the additional opportunity for submissions referred to here was to address the interpretation of Article 83(3) GDPR in the EDPB Decision and its application to this Inquiry, not to reopen the question of the appropriate quantum for any administrative fine and/or to provide for an additional round of submissions on that issue. The Commission in any event rejects any suggestion that the Article 83(1) GDPR criteria are not met by the new fine on the application of the new interpretation of Article 83(3) GDPR, and as is seen in Section 9 above, I have given due consideration to this and to Facebook's submissions in this regard. I therefore remain satisfied that the proposed application of Article 83(3) GDPR is consistent with Article 83(1) GDPR, for the reasons set out here and in Section 9.

10.20 In relation to the alleged contravention of the *ne bis in idem* principle, I also reiterate the views expressed at the end of Section 9 herein. It sets out that the failure to provide required information, and the failure to set out required information in a transparent manner, are entirely different wrongs. The legislator has provided for two distinct requirements, and each individual requirement has been infringed by Facebook. For these reasons and the reasons set out above, I

[151] *Ibid*, paragraph 5.6.
[152] *Ibid*, paragraph 5.10.
[153] *Ibid*, paragraph 5.11
[154] *Ibid*, paragraph 5.12.

do not accept this submission. Similarly, the Commission is not applying a new and retroactive view of wrongdoing to the conduct in a manner envisaged by principle of concurrence of laws. It is simply determining the proper interpretation of Article 83(3) GDPR. This has no impact on the Commission's detailed consideration of Facebook's submissions on the separate and more general question of the appropriate penalty.

10.21 It also argues that the taking into account of the undertaking's turnover is incorrect as a matter of law, as it is not set out as a factor in Article 83(2) GDPR. In this regard, the Commission relies on its existing analysis of its obligations to cooperate with the concerned supervisory authorities and apply the GDPR consistently. For the same reasons provided to support the Commission's decision to apply the EDPB Decision's interpretation of Article 83(3) GDPR in general, the Commission intends to maintain this consideration of the undertaking's turnover.

10.22 Finally, Facebook has argued that, in light of the intended Annulment Proceedings in respect of the WhatsApp Decision, the Commission should not finalise the Draft Decision until a final decision as to the correct interpretation of Article 83(3) GDPR has been made by the CJEU. Facebook's submission is simply that "*there is, at a minimum, very considerable doubt as to the correct interpretation of Article 83(3) GDPR*" and that on this basis the Commission should not proceed with this Draft Decision until the matter is finalised.[155] Facebook has provided no legal authority in support of this proposition. Notwithstanding the possible overlap between some of the questions referred and the issues arising for decision in this inquiry, given the advanced stage of this Inquiry I am satisfied that there is no reason to delay this matter. The prospect of intended legal proceedings in respect of a separate decision does not provide any basis in law for suspending a separate Inquiry.

ARTICLE 83(5) GDPR

10.23 Turning, finally, to Article 83(5) GDPR, I note that this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement, as follows:

> *"Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
> *…*
> *(b) the data subjects' rights pursuant to Articles 12 to 22;*
> *…"*

[155] *Ibid*, paragraph 6.3.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

10.24 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."*

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

> "*an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed"*[156].

10.26 The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement[157].

10.27 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.

10.28 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,

[156] *Höfner and Elser v Macrotron GmbH* (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161, paragraph 21.
[157] *Akzo Nobel and Others v Commission*, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, paragraphs 58 – 60.

organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case[158].

10.29 The CJEU has, however, established[159] that, where a parent company has a 100% shareholding in a subsidiary, it follows that: the parent company is able to exercise decisive influence over the conduct of the subsidiary; and a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

10.30 The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary[160].

10.31 The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise a decisive influence over the conduct of its subsidiary[161]. 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* …[162]"

10.32 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.

[158] *Ori Martin and SLM v Commission* (C-490/15 P, judgment delivered 14 September 2016) ECLI:EU:C:2016:678, paragraph 60.
[159] *Akzo Nobel and Others v Commission*, (C-97/08 P, judgment delivered 10 September 2009).
[160] Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, paragraph 48.
[161] 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.
[162] 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).

10.33 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.

10.34 I have noted already that Facebook's ultimate parent is Facebook Inc. I also note that Note 22 of the Financial Statements further confirms, on page 34, that:

> "*Controlling parties:*
>
> *At 31 December 2018, the company is a wholly-owned subsidiary of Facebook International Operations Limited, a company incorporated in the Republic of Ireland, its registered office being 4 Grand Canal Square, Grand Canal Harbour, Dublin 2.*
> *The ultimate holding company and ultimate controlling party is Facebook Inc., a company incorporated in Wilmington, Delaware, United States of America. The ultimate holding company and controlling party of the smallest and largest group of which the company is a member, and for which consolidated financial statements are drawn up, is Facebook, Inc.*"

10.35 On this basis, it is my understanding that Facebook is a wholly-owned subsidiary of Facebook International Operations Limited; Facebook International Operations Limited is wholly owned and controlled by Facebook Inc.; and, as regards any intermediary companies in the corporate chain, between Facebook and Facebook, Inc., it is assumed, by reference to the statement at Note 22 of the Notes to the Financial Statements (quoted above) that the "*ultimate holding company and controlling party of the smallest and largest group of which* [Facebook] *is a member … is Facebook, Inc.*". It is therefore assumed that Facebook, Inc. is in a similar situation to that of a sole owner as regards its power to (directly or indirectly) exercise a decisive influence over the conduct of Facebook.

10.36 It seemed therefore at the time of preparing the Preliminary Draft Decision, that the corporate structure of the entities concerned is such that Facebook Inc. is in a position to exercise decisive influence over Facebook's behaviour on the market. Accordingly, a rebuttable presumption will arise to the effect that Facebook Inc. does in fact exercise a decisive influence over the conduct of Facebook on the market.

10.37 If this presumption is not rebutted, it would mean that Facebook, Inc. and Facebook 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 Articles 83(4) and (5) GDPR, would fall to be determined by reference to the combined turnover of Facebook and Facebook Inc. Facebook has made submissions in this regard in an attempt to rebut the presumption of decisive influence.

10.38 In particular, Facebook submitted that the presumption of decisive influence on the market does not translate into a data protection context without considering what "behaviour on the market" means in a data protection context.[163] It argues that this analysis should focus instead on the entity that has the decision-making capacity in the context of data protection matters, rather than matters relating to the market in general as is the case in competition law. I do not agree with this assessment. Firstly, the suggested approach (involving an assessment of where the decision-making power lies, in relation to the processing of personal data) is effectively a replication of the assessment that must be undertaken at the outset of the inquiry process, the outcome of which determines (i) the party/parties to which the inquiry should be addressed; and (ii) (in cross border processing cases) the supervisory authority with jurisdiction to conduct the inquiry. Given the consequences that flow from this type of assessment, it would not be appropriate for this assessment to be conducted at the decision-making stage of an inquiry.

10.39 Secondly, the suggested approach could not be applied equally in each and every case. Where, for example, the presumption of decisive influence has been raised in the context of a cross-border processing case where one of the entities under assessment is outside of the EU, an assessment of that entity's ability to exercise decisive influence over the respondent's data processing activities would likely exceed 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".

10.40 Finally "behaviour on the market" has a meaning normally ascribed to it in EU competition law. In summary, "behaviour on the market" describes how an entity behaves and conducts its affairs in the context of the economic activity in which it engages. Such behaviour will include matters such as the policies and procedures it implements, the marketing strategy it pursues, the terms and conditions attaching to any products or services it delivers, its pricing structures, etc. I therefore can see no basis in law, in Facebook'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.

10.41 Applying the above to Article 83(5) GDPR, I first 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 Facebook Inc. reported the generation of revenue in the amount of $84.169 billion in respect of the year ended 31 December

[163] Facebook Submissions on Preliminary Draft Decision, paragraph 16.2.

NOTE: Compare the DPC's summaries of the submissions by the complainant against the relevant documents, as arguments are partly missing, not accurately reflected or taken out of context.

2020. That being the case, the fine proposed above does not exceed the applicable fining "cap" prescribed by Article 83(5) GDPR.

SUMMARY OF ENVISAGED ACTION

10.42 I therefore impose the following:

- An order, pursuant to Article 58(2)(d) GDPR, to bring the Data Policy and Terms of Service into compliance with Articles 5(1)(a), 12(1) and 13(1)(c) GDPR as regards information provided on data processed pursuant to Article 6(1)(b) GDPR, in accordance with the principles set out in this Draft Decision. It is proposed that this should be done within **three months** of the date of notification of any final decision.

- An administrative fine pursuant to Articles 58(2)(i) and 83 GDPR, of and amount not less than €28 million and an amount not more than €36 million.