In the matter of the General Data Protection Regulation

DPC Inquiry Reference: IN-20-8-1

In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited)

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation

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

DECISION

Decision-Maker for the Commission:

Helen Dixon

Commissioner for Data Protection

Dated the 12th day of May 2023

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

LIST OF ABBREVIATIONS

The following abbreviations appear in this Decision:

Abbreviation:	**Used to Denote:**
the 2018 Act	The Data Protection Act, 2018
The Article 60 Process	The cooperation procedure set out in Article 60 GDPR
The Article 65 Decision	The EDPB Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted 13 April 2023
The Article 65 Submissions	Meta Ireland's submissions, dated 2 November 2022, on the material that the DPC proposed to put before the EDPB for the purpose of the Article 65 Process
the Board	The European Data Protection Board
the Charter	Charter of Fundamental Rights of the European Union
the CJEU	Court of Justice of the European Union
the DPC	Data Protection Commission (previously the Data Protection Commissioner prior to the entry into application of the Data Protection Act, 2018)
the Commissioner	Data Protection Commissioner established pursuant to the Data Protection Acts, 1988–2003
the Complaint	Complaint filed by Mr Maximillian Schrems on 25 June 2013 as reformulated and resubmitted on 1 December 2015, and as re-scoped in the context of the settlement of the judicial review proceedings referenced at paragraph 2.45 below.
the CSAs	the supervisory authorities concerned, as defined by Article 4(22) GDPR

the Data Policy	Meta Ireland's Data Policy (available at: *https://www.facebook.com/policy.php*)
the Data Transfers	EU-US transfers of personal data relating to Users, made between Meta Ireland and Meta US
the Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
the Draft Decision	the draft version of this decision that was circulated to the CSAs for their views, in accordance with Article 60(3) GDPR
2015 DTPA	Meta US's Data Transfer and Processing Agreement, dated 20 November 2015
2018 DTPA	Meta US's Data Transfer and Processing Agreement, dated 25 May 2018
2021 DTPA	Meta US's Data Transfer and Processing Agreement, dated 27 August 2021
the EDPB	The European Data Protection Board
EO 12333	Executive Order 12333
The Final Submissions	Meta Ireland's submissions dated 8 May 2023 in relation to any matters in relation to which the DPC was required to make a final determination or, otherwise, exercise its own discretion, arising from the Article 65 Decision.
FISA	Foreign Intelligence Surveillance Act, 1978
FISC	Foreign Intelligence Surveillance Court
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with

	regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
the High Court Judgment	Judgment of the High Court delivered on 3 October 2017 (slightly revised 12 April 2018) ([2017] IEHC 545)
the High Court Proceedings	Proceedings commenced by way of plenary summons on 31 May 2016 under High Court Record No. 2016/4809 P
the Inquiry	The inquiry commenced by the Preliminary Draft Decision pursuant to Section 110 of the 2018 Act
the Judgment	Judgment in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* EU:C:2020:559
the Judicial Review	The application for judicial review brought by Meta Ireland in respect of the PDD, issued on 10 September 2020 (Record No: 2020/617 JR)
Meta Ireland	Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)
Meta US	Meta Platforms, Inc. (formerly Facebook, Inc.)
NSA	US National Security Agency
the PDD	The Preliminary Draft Decision delivered by the DPC herein on 28 August 2020
PPD-28	Presidential Policy Direction-28
the Prior Draft Decision	A draft decision issued by the DPC on 24 May 2016, prior to the commencement of the High Court Proceedings
Privacy Shield Decision	Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield ([2016] OJ L207/1)
the RPDD	The Revised Preliminary Draft Decision delivered by the DPC herein on 21 February 2022

Safe Harbour Decision	Decision 520/2000/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)
SCCs	Standard contractual clauses
the 2010 SCCs	Standard contractual clauses contained in the Annex to Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 ([2010] OJ 2010 L39/5), (subsequently amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 ([2016] OJ L344/100))
the 2010 SCC Decision	Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 ([2010] OJ 2010 L39/5), (subsequently amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 ([2016] OJ L344/100))
the 2021 SCCs	The standard contractual clauses contained in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
the 2021 SCC Decision	Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
the SRR	Meta US's Statement of Rights and Responsibilities (available at: *https://www.facebook.com/legal/terms/previous*

the Transparency Report	Meta US's Transparency Report (available at: https://transparency.fb.com/data/government-data-requests/country/US/)
TIA	Transfers Impact Assessment (Version 3.0) dated 31 August 2021 prepared by or on behalf of Meta Ireland and Meta US under and in accordance with Clause 14 of the 2021 SCCs.
US	The United States of America
USG	United States Government
Users	Individuals who are in the European Union/ European Economic Area who visit, access, use or otherwise interact with products and services provided by Meta Ireland, each of whom is a "data subject" for the purposes of Article 4(1) GDPR to the extent that their personal data is processed by Meta Ireland

1. INTRODUCTION

Preliminary Matters

Change of Name, Facebook Ireland Limited and Facebook, Inc.

1.1 On 11 January 2022, the DPC was notified that, effective from 5 January 2022, Facebook Ireland Limited, being the Respondent to the within inquiry, had changed its name to Meta Platforms Ireland Limited ("**Meta Ireland**"). In the circumstances, and for ease of reference, this decision refers to the Data Controller as "**Meta Ireland**" rather than Facebook Ireland Limited or FB-I, even where, at the relevant point in time, the Respondent's name was Facebook Ireland Limited. That is to say, references to "Meta Ireland" are to be taken to mean Facebook Ireland Limited where the context or timing of the matters to which reference is made so requires.

1.2 Facebook, Inc., being Meta Ireland's ultimate parent company and the recipient and/or importer of the personal data the subject of the data transfers under examination in the within inquiry, likewise changed its name, to Meta Platforms, Inc. Throughout this decision, I refer to this particular entity as "**Meta US**". In the circumstances, references to "Meta US" are to be taken to mean Facebook, Inc. where the context or timing of the matters to which reference is made so requires.

Purpose of this Document

1.3 This document is a decision ("**Decision**") of the Data Protection Commission ("the **DPC**"), delivered in the context of an own-volition inquiry ("the **Inquiry**"), commenced by the DPC pursuant to Section 110 of the Data Protection Act, 2018 ("the **2018 Act**") to consider the following two issues:

(1) Whether Meta Ireland is acting lawfully, and in particular, compatibly with Article 46(1) GDPR, in making transfers ("the **Data Transfers**") of personal data relating to individuals who are in the European Union/ European Economic Area who visit, access, use or otherwise interact with products and services provided by Meta Ireland, each of whom is a "data subject" for the purposes of Article 4(1) GDPR ("**Users**") to Meta US pursuant to standard contractual clauses ("the **2010 SCCs**") based on the clauses

set out in the Annex to Commission Decision 2010/87/EU[1] ("the **2010 SCC Decision**"), following the judgment of the Court of Justice of the European Union ("the **CJEU**"), delivered on 16 July 2020, in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* EU:C:2020:559 ("the **Judgment**"); and

(2) Whether and/or which corrective power should be exercised by the DPC pursuant to Article 58(2) GDPR in the event that the conclusion is reached that Meta Ireland is acting unlawfully and infringing Article 46(1) GDPR.

1.4 It should be noted that, subsequent to the commencement of the inquiry, the 2010 SCC Decision was repealed by the 2021 SCC Decision, whereupon the 2010 SCCs were replaced by the 2021 SCCs. As will be apparent from the terms of this Decision, the DPC's analysis herein has regard to both the 2010 SCCs and the 2021 SCCs. It also has regard to the 2021 DTPA, being an agreement entered into between Meta Ireland and Meta US, grounding the Data Transfers on the 2021 SCCs in place of the 2010 SCCs with effect from 31 August 2021.

Progression of the decision-making process

1.5 In circumstances where the processing under examination by way of the within inquiry constitutes "cross-border processing" for the purpose of Article 4(23) GDPR, the DPC was required, by Article 56(1) GDPR, to conclude this Decision in accordance with the procedure set out in Article 60 GDPR ("the **Article 60 Process**"). The Article 60 Process provides for a cooperation procedure, the purpose of which is to facilitate the conclusion of decisions on the basis of consensus between the lead supervisory authority ("the **LSA**") (in this case, the DPC) and any supervisory authorities concerned (as defined by Article 4(22) GDPR) ("the **CSAs**"). The Article 60 Process enables the CSAs to share their views with the LSA, including by way of a "relevant and reasoned objection". Where such an objection is raised to the LSA's draft decision during the Article 60 consultation period, the LSA must, if it does not "follow" the objection or is of the opinion that it is not relevant and reasoned, submit the matter to the European Data Protection Board (the "**Board**" or, otherwise, the "**EDPB**") for determination pursuant to the Article 65 GDPR dispute resolution process.

[1] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 ([2010] OJ 2010 L39/5), (subsequently amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 ([2016] OJ L344/100)).

1.6 During the course of the within Inquiry, a preliminary draft decision ("the **PDD**"), and subsequently a revised preliminary draft decision ("the **RPDD**") were provided to Meta Ireland, Mr. Maximilian Schrems ("**Mr. Schrems**") and the Government of the United States of America ("the **USG**") for the purpose of allowing them to make submissions in relation to my provisional findings. The DPC considered the submissions so made and, where necessary, made amendments to take account of these prior to the finalisation of a draft decision which was circulated to the CSAs, for the purpose of the Article 60 Process, on 6 July 2022 ("the **Draft Decision**").

1.7 The cross-border processing under examination was such that all other EU/EEA supervisory authorities ("**SAs**", each one being an "**SA**") were engaged as CSAs for the purpose of the Article 60 Process. Following the circulation of the Draft Decision to the CSAs for the purpose of enabling them to express their views, in accordance with Article 60(3) GDPR, objections were raised by the SAs of Austria, France, Hamburg (acting on behalf of all German SAs) and Spain. A number of comments were also exchanged by various CSAs.

1.8 Having considered the matters raised, the DPC, by way of a composite response memorandum dated 28 September 2022, set out its responses to the various objections and comments. Ultimately, it was not possible to reach consensus with the CSAs on the subject-matter of the objections and, accordingly, the DPC determined that it would not follow them and/or that they were not relevant and reasoned. In the circumstances, the DPC referred the objections to the EDPB for determination pursuant to the Article 65(1)(a) dispute resolution mechanism. In advance of doing so, the DPC invited Meta Ireland to exercise its right to be heard in relation the matters to be determined by the EDPB. Meta Ireland exercised its right to be heard by way of its submissions dated 2 November 2022 ("the **Article 65 Submissions**").

1.9 The EDPB determined the merits of the objections that were referred to it by way of a decision that it adopted on 13 April 2023. The EDPB notified its decision to the DPC all other CSAs on the same date. Further to Article 65(2) GDPR, the EDPB's decision is binding upon the DPC and all CSAs. Article 65(6) GDPR required the DPC to adopt its final decision "*on the basis of*" the EDPB's decision within one month after notification of the EDPB's decision. As part of the finalisation process, Meta Ireland was invited to exercise its right to be heard in relation to any matters in relation to which the DPC was required to make a final determination or, otherwise, exercise its own discretion. Meta Ireland exercised its right to be heard by way of its submissions furnished under cover of letter dated 8 May 2023 ("the **Final Submissions**"), which have been taken into account in this Decision.

1.10 Accordingly, this Decision further reflects the binding decision that was adopted by the EDPB on 13 April 2023 pursuant to Article 65(2) GDPR[2] ("the **Article 65 Decision**"), which directed that changes be made to certain of the positions reflected in the Draft Decision, as detailed further below. The Article 65 Decision will be published on the website of the Board, in accordance with Article 65(5) GDPR, and a copy of same is attached as the Schedule to this Decision.

Context of the Decision

1.11 Whilst issued in the context of the Inquiry, the Decision addresses issues arising in the context of the Judgment, and more particularly, in the context of the lengthy proceedings leading to the Judgment, which were commenced in the High Court on 31 May 2016 ("**the High Court Proceedings**"), and in which multiple parties participated, voluminous factual and expert evidence was adduced, and extensive legal submissions were made. Reference is also made in this connection to a judicial review application[3] issued by Meta Ireland ("the **Judicial Review**") challenging a Preliminary Draft Decision delivered by the DPC on 28 August 2020 ("the **PDD**").

Scope of the Inquiry

1.12 On 2 July 2021, Meta Ireland made certain observations in its written response to the PDD ("the **Response to the PDD**") regarding the scope of the Inquiry.[4]

1.13 For the avoidance of doubt, the DPC reiterates that Meta Ireland is correct in its understanding of the scope of the Inquiry. As such, it is correct that:

(1) the Inquiry, and this Decision, relate to the Facebook Service only (as defined by Meta Ireland in the Response to the PDD);

(2) the geographical scope of the Inquiry is limited to Users of the Facebook Service in the EU/EEA;

[2] Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service.
[3] High Court Record No. 2020 / 697 JR.
[4] Response to the PDD, Part B, paragraph 2.2.

(3) the substantive scope of the Inquiry relates to transfers pursuant to the 2010 SCC Decision and 2010 SCCs, and to transfers now taking place pursuant to the 2021 SCC Decision and the 2021 SCCs.

Summary

1.14 For the reasons set out below, and having carefully considered the submissions made by Meta Ireland, Mr. Schrems and the USG, respectively, in response to the PDD, and in response to the Revised Preliminary Draft Decision of 21 February 2022 ("the **RPDD**"), it is my view that, given the findings of the CJEU in the Judgment and all of the circumstances of which the DPC is aware:

(1) The Data Transfers are made in circumstances which fail to guarantee a level of protection to data subjects that is essentially equivalent to that provided by EU law, and in particular, by the GDPR read in light of the Charter of Fundamental Rights of the European Union ("the **Charter**"), and, accordingly, in making the Data Transfers, Meta Ireland is infringing Article 46(1) GDPR;

(2) Meta Ireland is not entitled to rely on any derogation under Article 49(1) GDPR in respect of the Data Transfers;

(3) It is both necessary and appropriate that I would order that the Data Transfers be suspended, pursuant to the DPC's powers under Article 58(2)(j) GDPR;

(4) Further to the determination of the EDPB set out at paragraph 267 of the Article 65 Decision, and as detailed further at Section 9 below, I will also, by way of this Decision, order Meta Ireland to bring its processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR; and

(5) Further to the determination of the EDPB set out at paragraph 142 of the Article 65 Decision, and detailed further at Section 9 below, I will also, by way of this Decision, impose an administrative fine in the amount of €1.2 billion on Meta Ireland in respect of the finding of infringement of Article 46(1) GDPR.

Sources

1.15 In formulating the views expressed in this Decision, and in making the findings contained herein, I have had regard to a range of material.

The Judgment

1.16 I have paid careful and close attention to the findings in the Judgment, which are binding on the DPC.

Submissions in response to the PDD

1.17 I have also paid careful and close attention to (i) the lengthy and detailed submissions made by Meta Ireland in its Response to the PDD; and (ii) its supplemental submissions dated 1 September 2021 and 20 September 2021 (together referred to as "the **Supplemental Response to the PDD**"), as well as the multiple Annexures accompanying same.

1.18 The Annexures to the Response to the PDD comprise the following:

(1) Transfer Impact Assessment Summary;

(2) Factors Assessment;

(3) Meta Ireland's Essential Equivalence Assessment of US Laws and Practice version 3.0 (draft);

(4) Meta Ireland's Record of Safeguards, including supplementary measures, version 3.0 (draft);

(5) Meta Ireland's Data Transfers Report dated 2 July 2021;

(6) Expert report of Professor Goldfarb dated 2 July 2021;

(7) Expert opinion of Geoffrey Robertson QC dated 2 July 2021;

(8) Relevant extracts from:

(a) Judicial Review, Statement of Opposition

(b) Judicial Review, Meta Ireland Replying Affidavit

(c) Judicial Review, DPC Replying Affidavit

(d) Judicial Review, DPC Response

(e) Judicial Review, Judgment

(9) Data Transfer and Processing Agreement between Meta Ireland and Meta US;

(10) US Government White Paper;

(11) Letter from the ICO to the SEC dated 11 September 2020;

(12) DPC letter to the LIBE Committee dated 9 February 2021;

(13) DPC letter to the LIBE Committee dated 12 March 2021;

(14) Deloitte Report;

(15) Copenhagen Report;

(16) SMB Surveys;

(17) May 2021 Transparency Update;

(18) November 2020 Transparency Update;

(19) Transfers Blog Post;

(20) Government Requests and Transfers FAQs;

(21) Kearney Report;

(22) Analysis Group Report.

1.19 The Annexures to the Supplemental Response to the PDD comprise:

(1) Data Transfer and Processing Agreement dated 31 August 2021;

(2) Redacted version of the Data Transfer and Processing Agreement dated 31 August 2021;

(3) Transfer Impact Assessment Summary (version 3.0);

(4) Factors Assessment (version 3.0);

(5) Equivalence Assessment (version 3.0);

(6) Record of Safeguards (version 3.0); and

(7) Modified Record of Safeguards identifying information requested by the DPC.

1.20 I have also had regard to the submissions filed by Mr. Schrems in response to the PDD, dated 15 August 2021 ("**Schrems' Submissions on the PDD**") and the submissions of the USG, likewise directed to the PDD, dated 20 September 2021.

1.21 I have also had regard to the expert report entitled *'Technical Report on Why EU-US Transfers Are Necessary to Provide the Facebook Service; Expert Report of Jason Nieh'* dated 24 September 2021 which was submitted by Meta Ireland as part of its reply to Schrems' Submissions on the PDD, received by the DPC on 24 September 2021. The full set of documents submitted by Meta Ireland along with its reply to the Schrems' Submissions on the PDD comprised the following:

(1) Annex 1 - Supplemental FIL Data Transfers Report;

(2) Annex 2 - Expert Report of Jason Nieh - September 24 2021;

(3) Appendix 1 - CV of Professor Jason Nieh;

(4) Appendix 2 - Shalita 2016 _ Social Hash an Assignment Framework for Optimizing Distributed Systems Operations on Social Networks;

(5) Appendix 3 - Bronson 2013_TAO Facebooks Distributed Data Store for the Social Graph;

(6) Appendix 4 - Shi 2020_FlightTracker Consistency across Read-Optimized Online Stores at Facebook;

(7) Appendix 5 - Large-scale graph partitioning with Apache Giraph - Facebook Engineering; and

(8) Appendix 6 - Annamalai 2018 _ Sharding the Shards Managing Datastore Locality at Scale with Akkio.

Submissions in response to the RPDD

1.22 I have also paid careful and close attention to the following submissions made by each of Mr Schrems, the USG, and Meta Ireland in response to the RPDD:

(1) Mr Schrems' submissions in response to the RPDD, received on 21 March 2022 ("**Schrems' Submissions on the RPDD**");

(2) The USG's submissions in response to the RPDD, received on 4 April 2022 ("**the USG's Response to the RPDD**"); and,

(3) Meta Ireland's submissions in response to the RPDD, received on 29 April 2022 ("**the Response to the RPDD**").

1.23 I have additionally taken account, when finalising this Decision, of the determinations made by the EDPB in the Article 65 Decision as well as Meta Ireland's Article 65 Submissions and Final Submissions.

Section 111 of the 2018 Act

1.24 I note that Meta Ireland refers to Section 111 of the 2018 Act and asserts that a decision "*can only be reached on the basis of 'information obtained in the inquiry'*".[5] As will be apparent from the contents of this Decision, I can confirm that, in terms of factual information, I have had regard only to factual information advanced by Meta Ireland in the Response to the PDD, the Supplemental Response to the PDD, the Response to the RPD, the Article 65 Submissions and the Final Submissions. Insofar as reference is made to any factual information not derived from the Inquiry, any such information does not appear to be in dispute. However, for the avoidance of doubt, I do not read Section 111 of the 2018 Act as precluding the DPC from having regard to the jurisprudence of the CJEU. Nor indeed could it so preclude the DPC.

Structure

1.25 In this Decision, I address the following in turn:

(1) A summary of the factual and procedural background to the Judgment;

(2) The functions and powers of the DPC relevant to the Inquiry;

[5] Response to the PDD, Part A, paragraph 2.4(E); Part B, paragraph 2.4.

(3) The DPC's position as the lead supervisory authority;

(4) The legal provisions regulating the Data Transfers;

(5) The current factual position regarding the Data Transfers;

(6) My findings on the question as to whether or not the Data Transfers give rise to one or more infringements of relevant provisions of the GDPR;

(7) My findings on whether Meta Ireland is entitled to rely on any of the derogations provided for by Article 49 GDPR; and

(8) My findings on whether and which corrective powers should be exercised.

2. FACTUAL AND PROCEDURAL BACKGROUND TO THE JUDGMENT AND THE INQUIRY

2.1 The factual and procedural background to the Judgment is complex and lengthy and will only be summarised here.

EU-US Data Transfers

2.2 On 26 July 2000, the European Commission adopted Decision 520/2000/EC ("the **Safe Harbour Decision**"),[6] establishing the so-called "*safe harbour*" arrangements for EU-US data transfers.

2.3 While the Safe Harbour Decision did not recognise the US as a third country which ensured "*an adequate level of protection*" for the purposes of Article 25(6) of Directive 95/46/EC ("the **Directive**"),[7] it nonetheless provided that EU-US transfers were permissible under its terms, provided the entity to whom the data was being transferred self-certified that it complied with: the safe harbour privacy principles; and a set of "*frequently asked questions*", both published by the US Department of Commerce and incorporated into the Safe Harbour Decision at Annexes 1 and 2 thereof.

2.4 Over time, the safe harbour arrangements became the primary mechanism by which data controllers established in the EU sought to legitimise data transfers to the US.

[6] Decision 520/2000/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Snowden Document Disclosure

2.5 In June 2013, Edward Snowden, a contractor engaged through a third party to undertake work for the US National Security Agency ("**NSA**"), disclosed documents revealing the existence of one or more programmes operated by the NSA under which internet and telecommunications systems operated by some of the world's largest technology companies, including, by way of example, Microsoft, Apple, Meta US, and others, were the subject of surveillance programmes.

The Complaint

2.6 On 25 June 2013, Mr Schrems filed the Complaint with the Data Protection Commissioner ("the **Commissioner**"). In essence, the Complaint contended that, in light of the Snowden document disclosure, the transfer of personal data relating to (Meta US's European Users) by Meta Ireland to its US parent, Meta US, was unlawful under both national and EU data protection law. In practical terms, the Complaint sought to mount a full-frontal challenge to the Safe Harbour Decision.

2.7 On receipt of the Complaint, the (then) Commissioner took the view that, in circumstances in which the European Commission had adopted the Safe Harbour Decision establishing and/or endorsing the safe harbour arrangements, the Commissioner was bound to accept that decision as binding upon him in light of Article 25(6) of the Directive and Section 11(2) of the Data Protection Acts, 1988 and 2003. Accordingly, the Commissioner declined to investigate the Complaint, deeming it unsustainable in law.

2.8 That position was challenged by Mr Schrems by way of an application for judicial review commenced on 21 October 2013. In that application, orders were sought that would quash the Commissioner's refusal to investigate and to direct the Commissioner to investigate and decide the Complaint on its merits.

European Commission Response to the Snowden Document Disclosure

2.9 In response to concerns expressed by the European Commission arising from the Snowden document disclosure, the US agreed to participate in an *ad hoc* EU/US Working Group established in July 2013 to facilitate a fact-finding exercise by the European Commission under which the European Commission would be afforded an opportunity to seek clarifications on the scope of the programmes revealed by Mr Snowden, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to

individuals in the EU, and the different levels of protection and procedural safeguards that apply to persons in the US and EU/EEA respectively.

2.10 On 27 November 2013, the European Commission published a report setting out the findings of the EU Co-Chairs of the ad hoc EU/US Working Group. Among other things, the report noted that, in the course of the Working Group's discussions, the US had confirmed the existence of the PRISM programme, identifying it as a programme authorised and/or operated under Section 702 of the Foreign Intelligence Surveillance Act 1978 ("**FISA**").

2.11 More specifically, the US was recorded as having confirmed that, on the basis of Section 702 FISA, electronically stored data, including content data, was collected *"by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube."*

2.12 The report proceeded to make the following points:

(1) *"The US also confirmed that Section 702 provides the legal basis for so-called 'upstream collection'; this is understood to be the interception of Internet communications by the NSA as they transit through the US (e.g. through cables, at transmission points).*

Section 702 does not require the government to identify particular targets or give the Foreign Intelligence Surveillance Court (hereafter 'FISC') a rationale for individual targeting. Section 702 states that a specific warrant for each target is not necessary";[8]

(2) "*The US stated that no blanket or bulk collection of data is carried out under Section 702, because collection of data takes place only for a specified foreign intelligence purpose.*"[9]

2.13 Under the heading "*Summary of Main Findings*", the report identified a number of concerns regarding US law, including the following:

[8] Report, paragraph 2.1.1.
[9] Report, paragraph 2.1.1.

(1) Under US law, "*a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies*";[10]

(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, including that targeting and minimisation procedures approved by the Foreign Intelligence Surveillance Court ("**FISC**") are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons and do not apply to the personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity, while US persons benefit from constitutional protections, such as the Fourth Amendment, that do not apply to EU citizens not residing in the US;

(3) Under US surveillance programmes, different levels of data protection apply to different types of data (Meta US-data versus content data) and different stages of data processing (initial acquisition versus further processing/analysis);

(4) There is a lack of clarity as the use of other legal bases and the applicable limitative conditions, especially regarding Executive Order 12333 ("**EO 12333**"); and,

(5) There were no avenues for either EU or US data subjects to be informed of whether their personal data was being collected or further processed, and no opportunities to obtain access, rectification, or erasure of data.

2.14 On the same date, the European Commission published a separate document titled "*Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*." [11]

2.15 The document made 13 specific recommendations in relation to changes the European Commission considered would need to be made to the safe harbour arrangements in the context of ongoing negotiations with the US.

[10] Report, paragraph 5(1).
[11] COM (2013) 847 Final.

Judgments in the Application for Judicial Review

2.16 On 29 April 2014, Mr Schrems' application for judicial review came on for hearing in the High Court.

2.17 On 18 June 2014, judgment was delivered by The Hon. Mr. Justice Gerard Hogan. While the High Court found that, in coming to the view that he was bound to apply the Safe Harbour Decision, the (then) Commissioner had steadfastly applied the law as it existed at that point, Mr. Justice Hogan nonetheless determined that it would be appropriate to refer a number of questions to the CJEU so that the CJEU could in turn determine, in particular, whether the Commissioner was bound, absolutely, by the Safe Harbour Decision having regard to Articles 7, 8 and 47 of the Charter, the provisions of Article 25(6) of the Directive notwithstanding.

2.18 On 6 October 2015, the CJEU delivered its judgment (Case C-362/14 *Schrems v Data Protection Commissioner* EU:C:2015:650) ("the **Judgment in Case C-362/14**"). While noting that the CJEU alone has jurisdiction to declare an EU act invalid, and that, until such time as the Safe Harbour Decision was declared invalid by the Court, the Commissioner was not at liberty to adopt any measure contrary to its terms, the CJEU nonetheless found that, as a matter of EU law, the Safe Harbour Decision did not preclude the conduct of an investigation into EU-US data transfers by the Commissioner so that the Commissioner ought properly to have investigated the Complaint with all due diligence.

2.19 The CJEU also concluded that, as a matter of EU law, the Safe Harbour Decision was invalid.

2.20 Mr Schrems' application for judicial review came back before the High Court, and on 20 October 2015, an Order was made by Mr. Justice Hogan quashing the Commissioner's refusal to investigate the Complaint and remitting the Complaint back to this Office for investigation.

Post-Litigation Investigation of the Complaint

2.21 Immediately thereafter, the Commissioner opened an investigation into the Complaint.

2.22 In circumstances in which there was by now no question but that EU-US transfers of Users' personal data could no longer be undertaken under the Safe Harbour Decision, the investigation sought to establish whether, following the demise of the Safe Harbour Decision, the transfer of personal data relating to Users by Meta Ireland to Meta US was lawful. To that end, the Commissioner set out to examine (by reference to the Complaint as it relates to interferences on national security grounds with citizen's data privacy rights):

(1) Whether, by reference to the adequacy criteria identified in Article 25(2) of the Directive, the US ensured adequate protection for the data protection rights of EU citizens; and,

(2) If and to the extent that the US does not ensure adequate protection, whether it was open to Meta Ireland to rely on one or more of the derogations provided for at Article 26 of the Directive to legitimise the transfer of Users' personal data to the US, if indeed, such transfers continue to take place.

2.23 By letter dated 3 November 2015, the Office of the Commissioner notified Meta Ireland of the commencement of the investigation.

2.24 Separately, Mr Schrems was invited to reformulate the Complaint so as to focus, not on the (now defunct) safe harbour arrangements, but on such derogations (if any) as may be relied on by Meta Ireland to legitimise data transfers to Meta US post-6 October 2015.

2.25 On 1 December 2015, Mr Schrems duly submitted his reformulated Complaint. Having secured access in the interim to one or more of the data processing agreements to which Meta Ireland and Meta US are party, the Complaint referred to the nature and extent of those parties' reliance on the 2010 SCC Decision. In particular, Mr Schrems made the following complaints:

> "*'Facebook Ireland Ltd' has not proven that [its] alternative agreement was authorized by the DPC under Section 10(4)(ix) DPA. Even if it would be, such an authorization would be invalid and void in the light of the judgments C-362/14 and Schrems –v- the Data Protection Commissioner and therefore irrelevant in this procedure.*
>
> *…*
>
> *Even if the current and all previous agreements between 'Facebook Ireland Ltd' and 'Facebook Inc' would not suffer from the countless formal insufficiencies above and would be binding for the DPC (which it is not), 'Facebook Ireland Ltd' could still not rely on them in the given situation of factual 'mass surveillance' and applicable US laws that violate Art 7, 8 and 47 of the CFR (as the CJEU has held) and the Irish Constitution (as the Irish High Court has held).*"

2.26 As the Judgment notes,[12] in the course of the Commissioner's investigation, Meta Ireland also confirmed that a large volume of Users' personal data was transferred to Meta US pursuant to the 2010 SCCs set out in the Annex to the 2010 SCC Decision.

Prior Draft Decision

2.27 On 24 May 2016, the Commissioner issued a "*draft decision*" ("the **Prior Draft Decision**") summarising the provisional findings of her investigation.

2.28 In the Prior Draft Decision, the Commissioner took the provisional view that the personal data of EU citizens transferred to the US were likely to be consulted and processed by the US authorities in a manner incompatible with Articles 7 and 8 of the Charter and that US law did not provide those citizens with legal remedies compatible with Article 47 of the Charter. The Commissioner also expressed a preliminary view that the 2010 SCCs in the Annex to the 2010 SCC Decision were not capable of remedying that defect, since they confer only contractual rights on data subjects against the data exporter and importer, without, however, binding the US authorities.

High Court Proceedings

2.29 Taking the view that, in those circumstances, the Complaint raised the issue of the validity of the 2010 SCC Decision in the context of the transfer of personal data from the EU/EEA to the US, the Commissioner issued proceedings in the High Court on 31 May 2016, relying on paragraph 65 of the Judgment in Case C-362/14, in order for the High Court to refer a question on that issue to the CJEU.

2.30 There followed complex and lengthy plenary proceedings before the High Court.

2.31 The detailed steps in the High Court Proceedings are too many to be reproduced in this Decision but an analysis of the evidence and submissions adduced in the High Court Proceedings can be found in the judgment of the High Court, delivered on 3 October 2017.

2.32 By way of very brief summary, the High Court Proceedings involved:

(1) Extensive participation by both Meta Ireland and Mr Schrems;

[12] Judgment, paragraph 54.

(2) Extensive participation of four amici curiae joined to the High Court Proceedings, namely, Business Software Alliance, Digital Europe, Electronic Privacy Information Centre, and the US;

(3) Voluminous factual and expert evidence, both oral and written;

(4) An exchange of 22 Affidavits, with a total of 60 tabbed exhibits/appendices;

(5) Evidence from five experts in US law, who were called and gave evidence over seven days in the High Court;

(6) Two Joint Expert Reports (with the second of the Joint Expert Reports being furnished following the conclusion of the High Court hearing and dealing with new developments in US law);

(7) Extensive oral and written legal submissions, with seven sets of legal submissions filed in advance of the High Court hearing and further speaking notes prepared and handed in to the Court during the course of the hearing;

(8) A substantive hearing which lasted 21 days;

(9) A further hearing on 1 June 2017 following conclusion of the substantive hearing, dealing with new developments in US law;

(10) Delivery of the High Court Judgment on 3 October 2017 ([2017] IEHC 545);

(11) A further detailed hearing on certain of the factual findings in the High Court Judgment and on the formulation of the reference questions, heard over 4 days, on 1 December 2017 and from 16-18 January 2018; and

(12) Issue of a very slightly revised version of the High Court Judgment on 12 April 2018.

2.33 Ultimately, by order of 4 May 2018, the High Court made a reference for a preliminary ruling to the CJEU, having refused an application by Meta Ireland to stay such order pending the appeal referred to below.

Supreme Court Appeal

2.34 On 11 May 2018, Meta Ireland appealed the High Court Judgment to the Supreme Court.

2.35 The hearing of the appeal took place over two and a half days on 21–23 January 2019.

2.36 On 31 May 2019, the Supreme Court issued its judgment, concluding that, while it had jurisdiction to overturn the findings of fact made in the High Court Judgment, there was no basis for doing so, despite Meta Ireland arguing the contrary.

2.37 Thus, the findings of fact in the High Court Judgment were fully endorsed by the Supreme Court.

CJEU Hearing and Judgment

2.38 The hearing before the CJEU took place on 9 July 2019, and involved the participation of:

(1) The Commissioner;

(2) Meta Ireland;

(3) Mr Schrems;

(4) British Software Alliance;

(5) Electronic Privacy Information Centre;

(6) Digital Europe;

(7) The US;

(8) Ireland;

(9) The Belgian Government;

(10) The Czech Government;

(11) The German Government;

(12) The French Government;

(13) The Netherlands Government;

(14) The Austrian Government;

(15) The Polish Government;

(16) The Portuguese Government;

(17) The United Kingdom Government;

(18) The European Parliament;

(19) The European Commission; and

(20) The EDPB.

2.39 As noted above, the Judgment was delivered on 16 July 2020.

PDD

2.40 Following review and careful consideration of the Judgment, the DPC commenced the Inquiry and issued the PDD to Meta Ireland under cover of letter on 28 August 2020.

2.41 The PDD notified Meta Ireland of the fact that the DPC was opening the Inquiry and outlined the DPC's preliminary views on the Data Transfers.

Judicial Review

2.42 On 10 September 2020, Meta Ireland commenced the Judicial Review against the DPC, following which a stay was put on the Inquiry by Order of the High Court (Meenan J.) made on 14 September 2020.

2.43 Following a hearing in December 2020, The Hon Mr. Justice Barniville issued judgment in the Judicial Review on 14 May 2021, dismissing the application. An Order lifting the stay on the Inquiry was subsequently made on 20 May 2021.

2.44 The DPC subsequently wrote to Meta Ireland on 21 May 2021 informing it that the Inquiry would now be reviewed and inviting it to make such submissions as it wished to make in response to the PDD no later than 2 July 2021.

Schrems' Judicial Review

2.45 Mr. Schrems also brought a separate application for judicial review against the DPC. Those proceedings[13] were struck out by Order of the Court made on 13 January 2021, settlement terms having been agreed between the parties pursuant to which, amongst other things, Mr

[13] High Court Record No. 2020 / 707JR.

Schrems agreed, firstly, that the investigation of the Complaint would be conducted separately and solely by reference to applicable provisions of the GDPR (to the exclusion of any consideration of the Complaint by reference to the Directive) and, secondly, that the temporal scope of the Complaint would be further revised so as to take 25 May 2018 as its starting point. (Prior to settlement, the DPC had already indicated to Mr Schrems that he would be afforded an opportunity to make submissions in the Inquiry)[14].

Submissions in response to the PDD

2.46 Meta Ireland submitted its Response to the PDD on 2 July 2021. As already set out above, those submissions were lengthy and detailed and included multiple appendices.

2.47 Schrems' Submissions on the PDD were received on 15 August 2021.

2.48 Following preliminary consideration of Meta Ireland's Response to the PDD, in correspondence dated 18 August 2021, the DPC raised a number of queries with Meta Ireland in relation to the Inquiry.

2.49 Meta Ireland initially responded in correspondence dated 18 August 2021, and subsequently submitted its Supplemental Response to the PDD on 1 September 2021 (with certain of the Appendices to the Supplemental Response being re-submitted on 24 September 2021).

2.50 The USG's Response to the PDD was received on 20 September 2021.

2.51 Meta Ireland replied to Schrems' Submissions on the PDD on 24 September 2021.

The RPDD

2.52 Having carefully considered the submissions received in response to the PDD, the DPC prepared and delivered its Revised Preliminary Draft Decision, or RPDD, on 21 February 2022.

2.53 Mr Schrems delivered his Submissions in response to the RPDD on 21 March 2022.

[14] On 21 May 2021, following the final order made in Meta Ireland's Judicial Review, the DPC served Mr. Schrems with the form of notice required under Section 108(1) of the 2018 Act. By further letters dated 18 June 2021, Meta Ireland and Mr. Schrems were notified of the commencement of a separate statutory inquiry, directed to the Complaint, as reconstituted pursuant to the Terms of Settlement entered into between the DPC and Mr. Schrems in respect of the Schrems' Judicial Review. A preliminary draft decision was later circulated to Mr. Schrems and Meta Ireland in respect of the Complaint on 28 February 2023. Further submissions having been received from both of those parties in the interim, the DPC duly submitted its Draft Decision to the cooperation procedure provided for at Article 60 GDPR on 11 April 2023.

2.54 The USG delivered its Response to the RPDD on 4 April 2022.

2.55 Meta Ireland Limited delivered its Response to the RPDD on 29 April 2022.

Other Matters

2.56 On 7 October 2022, the President of the United States signed Executive Order 14086 entitled "Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities" ("**EO 14086**"). On the same date, the US Attorney General signed Rule / Regulations 28 CFR 201, establishing, within the US Department of Justice, a "Data Protection Review Court" ("the **Regulations**").

2.57 In the context of the within Inquiry, the above events occurred at a point in time when the DPC had already determined it necessary to refer the objections that were raised by the CSAs during the Article 60 Process to the EDPB for determination.

2.58 Following the signing of EO 14086, Meta Ireland wrote to the DPC to request confirmation that the DPC would afford it a right to be heard in respect of the changes to US law and practice that were brought about by EO 14086 and the Regulations. It also requested the DPC to consider whether it was necessary to revise the Draft Decision, before making any referral to the Article 65 process, in light of the "material development" that had occurred.

2.59 For the purpose of considering Meta Ireland's requests, the DPC undertook an examination of EO 14086 and the Regulations, limited in its scope to an examination of the question as to whether and/or to what extent the new form of redress scheme contemplated by those documents had, in fact, come into operation.

2.60 By way of high level summary of the outcome of the DPC's examination, it appeared to the DPC that, pursuant to EO 14086 and the Regulations:

(1) Complaints will be received and reviewed under the new redress mechanism introduced by EO 14086 and the Regulations only where they originate in a designated "qualifying state".

(2) In this respect:

a. Sec. 3(a) of EO 14086 explains that the purpose of the section is to establish "a redress mechanism to review ***qualifying complaints*** transmitted by the

appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, appropriate remediation",[15]

b. An element of the definition of "qualifying complaint" is that it must come from a "qualifying state" (see Sec. 4 (k)(i));

c. Sec. 3(f) deals with designation of a qualifying state, and in particular, Sec. 3(f)(i) provides:

> "*To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that [the conditions specified in Sec. 3(f)(i)(A)—(C) are satisfied]*";

d. For its part, §201.1 of the Regulations provides:

> "*This part establishes an independent and impartial Data Protection Review Court (DPRC) to consider, in classified proceedings, applications for review of determinations made by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI CLPO) in response to* ***qualifying complaints*** *submitted through the redress mechanism established pursuant to section 3 of the Executive order of October 7, 2022, "Enhancing Safeguards for United States Signals Intelligence Activities*."[16]

e. §201.2 provides that:

> *"The terms "appropriate remediation," "covered violation," "element of the Intelligence Community," "Intelligence Community," "national security," and "qualifying complaint" shall have the same meanings as they have in the*

[15] Emphasis added.
[16] Emphasis added.

Executive order of October 7, 2022. The term "qualifying state" means a country or regional economic integration organization designated as a qualifying state by the Attorney General pursuant to section 3(f) of the Executive order of October 7, 2022."

(3) It is apparent from these provisions that the new redress mechanism can only be engaged by a "qualifying complaint", which, in turn, must originate in a state that has been designated as a "qualifying state". Critically, however, to date the EU has not been designated as a "qualifying state" (and indeed, to the DPC's knowledge, no designations at all have yet been made under Sec. 3(f) of EO 14086). On that basis, it is clear that the new redress mechanism introduced by EO 14086 and the Regulations is not accessible by EU citizens at this point in time.

(4) Even if all the other elements of the redress mechanism envisaged by EO 14086 and the Regulations had been fully and completely implemented (and for the reasons set out below, this does not appear to be the case), in the absence of designation of the EU as a "qualifying state", the new redress system is not capable of being invoked by an EU citizen.

(5) In any event, it appears that the other elements of the redress mechanism envisaged by EO 14086 and the Regulations have not in fact been fully and completely implemented. In this regard:

a. the redress scheme contemplated by EO 14086 and the Regulations is entirely self-contained and will operate by reference to the particular procedures and/or arrangements laid down in those documents. The DPC notes that Sec. 5(h) of EO 14086 delineates the scope and range of its application in the following terms:

"*This order creates an entitlement to submit qualifying complaints to the CLPO and to obtain review of the CLPO's decisions by the Data Protection Review Court in accordance with the redress mechanism established in section 3 of this order. This order is not intended to, and does not, create any other entitlement, right, or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers,*

employees, or agents, or any other person. This order is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law."

b. A provision similar to Sec. 5(h) is contained in the Regulations, described as a "disclaimer" and expressed in the following terms:

"§201.12 Disclaimer

This part governs the ability to obtain review of the ODNI CLPO's determinations by the [Data Protection Review Court ("DPRC")] DPRC in accordance with the redress mechanism established in section 3 of the Executive order of October 7, 2022. This part is not intended to, and does not, create any other entitlement, right, or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. This part is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law."

c. Sec. 3(b) of EO 14086 provides that, within 60 days of the date of its signing, a process for the submission of qualifying complaints will be established. It is unclear if such procedures have been adopted at this point.

d. Separately, Sec. 3(c)(i) of EO 14086 provides that "*the Director [of National Intelligence], in consultation with the Attorney General, shall establish a process that authorizes the CLPO to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints…*". Noting that no timeline appears to be fixed for its establishment, the DPC understands that this process has not in fact been established at this point.

e. Likewise, the guidance referred to at Sec. 5(f) of EO 14086 has not yet been adopted, being guidance intended to address "the scope of application" of the Executive Order with respect to individual elements of the US Intelligence

Community, and which is intended to be "authoritative and binding" on, inter alia, the Data Protection Review Court.

f. Additionally, the DPC notes that policies and procedures previously issued by each individual element of the US Intelligence Community under Presidential Policy Directive 28 (PPD-28) are to be updated, by means of a consultative procedure involving the US Attorney General, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence and the Privacy and Civil Liberties Oversight Board, in order to implement the particular safeguards for which provision is intended to be made in EO 14086. Under the terms of Sec. 2(c)(iv)(B) of EO 14086, that exercise is to be completed within a period of one year of the date of EO 14086. The DPC understands that it has not been completed to date. In the circumstances, the status quo ante remains intact, a point expressly affirmed at Section 2(c)(iv)(A) of the EO 14086.

g. No judges have yet been appointed to the new Data Protection Review Court in accordance with §201.3 of the Regulations (and Sec. 3(d)(i)(A) of EO 14086); it follows that the rules of procedure referenced at §201.3(d) of the Regulations have likewise not yet been adopted.

h. The "special advocates" referenced §201.4 of the Regulations (and Sec. 3(d)(i)(C) of EO 14086) have not yet been appointed.

2.61 The DPC's position – as outlined above (and as set out in a letter issued to Meta Ireland's legal advisors on 13 December 2022) – having been disputed by Meta Ireland, the DPC wrote again to Meta Ireland by letter dated 19 January 2023, reiterating its view that there had been no material change to the remedial scheme considered by the DPC in the Draft Decision. The DPC's letter also disputed the suggestion that EO 14086 and associated Regulations were effective and binding immediately upon the issuance of same. The DPC made the point that, on its terms, EO 14086 is directed to, and governs actions by, the US Intelligence Agencies. In circumstances where subsection 2(c)(iv)(A) explicitly provides that the Intelligence Agencies "shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities)(PPD-28), until they are updated pursuant to subsection (c)(iv)(B) of this section", and where subsection 2(c)(iv)(B) requires the Intelligence Agencies, over the course of one year, to consult with a range of third parties before completing the updating exercises to which reference is made, it could not credibly be

said that the activities and/or practices of the Intelligence Agencies are to be treated as having changed, materially, and immediately, on 7 October 2022; nor could it be said that the updating exercise demanded by the terms of the Executive Order itself is to be viewed as little more than an administrative tidy-up

2.62 The DPC also noted that the privacy and civil liberties safeguards introduced by EO 14086 do not appear to be intended to apply retrospectively, a point supported by the contents of the Implementation Procedures adopted by the Office of the Director of National Intelligence for the Signals Intelligence Redress Mechanism under Executive Order 14086 (Intelligence Community Directive 126, dated 6 December 2022.

2.63 In the circumstances, and fully reserving the DPC's position on the question as to whether, upon its full implementation, the remedial scheme contemplated by EO 14086 satisfies the requirements of Article 47 of the EU Charter on Fundamental Rights, it appears to the DPC that the scheme in question (both at the time the DPC carried out the review described above and at the date of adoption of this Decision) is not, in fact, operational. More particularly, and as explained above, in the absence of designation of the EU as a "qualifying state", the new scheme is not operational at all for EU citizens.

2.64 Against the background of the above, and having given careful consideration to the matters raised by Meta Ireland in its correspondence, the DPC concluded that:

a. At the time when the DPC carried out its review, the remedial scheme contemplated by EO 14086 was not, in fact, operational (this remains the case as at the date of adoption of this Decision). Nor had the activities and/or practices of the Intelligence Agencies changed, immediately upon signing of EO 14086, in a manner, or to such an extent, that it could be said that the analysis contained in the Draft Decision as it relates to Articles 7 and/or 8 of the Charter had been overtaken by events and is not inaccurate and/or incomplete. (Again, I am satisfied that that remains the case as of the date of this Decision).

b. Accordingly, the risk to the fundamental rights and freedoms of EU citizens pursuant to Article 47 of the Charter, as identified and discussed by the CJEU in the Judgment, has not yet been addressed.

c. While it is possible that the remedial scheme may yet become fully operational in the future, such that the deficiencies identified and discussed by the CJEU in the Judgment

might yet be addressed, the DPC is under an obligation to give effect to the law as it currently stands.

2.65 Accordingly, the DPC referred the CSA objections to the EDPB for determination pursuant to the Article 65 dispute resolution mechanism on 19 January 2023.

3. DPC'S FUNCTIONS AND POWERS RELEVANT TO THE INQUIRY

3.1 I now turn to the functions and powers of the DPC relevant to the Inquiry.

Charter

3.2 Under Article 8(3) of the Charter, compliance with Article 8 shall be subject to control by an independent authority.

GDPR

3.3 Under Article 51(1) GDPR, each Member State is required to provide for the establishment of one or more independent public authorities to be responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union, known as a "*supervisory authority*".

3.4 Pursuant to Article 55(1) GDPR, "*each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with [the GDPR] on the territory of its own Member State*".

3.5 Article 56(1) GDPR provides that, without prejudice to Article 55 GDPR, the supervisory authority "*of the main establishment or of the single establishment of the controller or processor*" shall be competent to act as "*lead supervisory authority for the cross-border processing*" carried out by that controller or processor in accordance with the procedure provided in Article 60 GDPR (emphasis added).

3.6 According to Article 57(1) GDPR, without prejudice to the other tasks set out in the GDPR, each supervisory authority shall, on its territory, in particular:

(1) "*monitor and enforce the application*" of the GDPR (Article 57(1)(a));

(2) "*cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of*" of the GDPR (Article 57(1)(g));

(3) "*conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority*" (Article 57(1)(h));

(4) "*monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices*" (Article 57(1)(i)); and

(5) "*fulfil any other tasks related to the protection of personal data*" (Article 57(1)(v)).

3.7 Article 58(2) GDPR provides that each supervisory authority shall have all of the following corrective powers:

"*(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

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

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such

actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

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

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation."

3.8 Meanwhile, Article 60 GDPR provides for a system of cooperation between the lead supervisory authority and the other supervisory authorities concerned.

3.9 Article 60(1) GDPR provides that the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with Article 60 GDPR in an endeavour to reach consensus and that the lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

3.10 Article 60(2) GDPR provides that the lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 GDPR and may conduct joint operations pursuant to Article 62 GDPR, in particular, for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3.11 Article 60(3) GDPR provides that the lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned and that it shall, without delay, submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

3.12 Article 60(4) GDPR provides that where any of the other supervisory authorities concerned within a period of 4 weeks after having been consulted in accordance with Article 60(3) GDPR, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion

that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63 GDPR.

3.13 Article 63 GDPR imposes an obligation on supervisory authorities to cooperate with each other, and where relevant, with the European Commission.

3.14 Article 65 GDPR provides that the EDPB may engage in dispute resolution, and in particular, pursuant to Article 65(1)(a) GDPR, that it may adopt a binding decision in a case referred to in Article 60(4) GDPR.

The 2018 Act

3.15 The 2018 Act was commenced on 25 May 2018. This legislation established, under Section 10, the DPC as the data protection supervisory authority in Ireland for the purposes of the GDPR.

3.16 Pursuant to Section 110 of the 2018 Act, the DPC may, "*of its own volition, in order to ascertain whether an infringement has occurred or is occurring, cause such inquiry as it thinks fit to be conducted for that purpose*".

3.17 Section 111 of the 2018 Act deals with the outcomes of an own volition inquiry under Section 110, and provides as follows:

> "*(1) Where an inquiry has been conducted of the Commission's own volition, the Commission, having considered the information obtained in the inquiry, shall –*
>
> *(a) If satisfied that an infringement by the controller or process to which the Inquiry relates has occurred or is occurring, make a decision to that effect, and*
>
> *(b) If not so satisfied, make a decision to that effect.*
>
> *(2) Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision –*
>
> *(a) As to whether a corrective power should be exercised in respect of the controller or processor concerned, and*

(b) Where it decides to so exercise a corrective power, the corrective power that is to be exercised.

(3) The Commission, where it makes a decision referred to in subsection (2)(b), shall exercise the corrective power concerned."

3.18 The application of Sections 110 and 111 of the 2018 Act in the context of the present inquiry is, of course, subject to Article 60 GDPR, in circumstances where, for the reasons set out below, it is my view that the processing at issue in the Inquiry constitutes cross-border processing, within the meaning of that term as defined at Article 4(23), GDPR.

3.19 Section 115(1) of the 2018 Act provides that, for the purposes of exercising a corrective power under Section 111, 112 or 113 of the 2018 Act, the DPC may do either or both of the following:

(1) Subject to Chapter 6, decide to impose an administrative fine on the controller or processor concerned (Section 115(1)(a));

(2) Exercise any other corrective power specified in Article 58(2) GDPR (Section 115(1)(b)).

3.20 Section 107 defines the term "*corrective power*" for the purpose of these provisions as "*a power conferred by Article 58(2)*" of the GDPR, to which reference has already been made above.

<u>The CJEU Consideration of the Functions of National Supervisory Authorities</u>

3.21 It is also important to note that the relevant functions and powers of the DPC as a statutory body were considered in the Judgment.

3.22 The CJEU noted[17] that, in accordance with Article 8(3) of the Charter and Articles 51(1) and 57(1)(a) GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data.

3.23 It further noted[18] that each of those authorities is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in the GDPR.

[17] Judgment, paragraph 107.
[18] Judgment, paragraph 107.

3.24 The CJEU added that it follows from those provisions that:

> "*the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement. The exercise of that responsibility is of particular importance where personal data is transferred to a third country since, as is clear from recital 116 of that regulation, 'when personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information'. In such cases, as is stated in that recital, 'supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders'*".[19]

[19] Judgment, paragraph 108.

4. DPC'S POSITION AS THE LEAD SUPERVISORY AUTHORITY

4.1 For the reasons that follow, I find that:

(1) In effecting the Data Transfers at issue, Meta Ireland, being a controller in the EU having establishments in more than one Member State, processes Users' personal data, and, further, that such processing constitutes "cross-border processing", as defined in Article 4(23) GDPR;

(2) In circumstances where the Data Transfers involve cross-border processing, it follows that the supervisory authority being competent to act as lead supervisory authority in respect of such processing for the purposes of Article 60 GDPR falls to be determined by reference to Article 56 GDPR; and,

(3) Having regard to the provisions of Article 56(1) GDPR, and in circumstances where Meta Ireland has its main establishment in Ireland, the DPC is properly to be considered the *"lead supervisory authority"* in respect of the Data Transfers.

Controller

4.2 It is not disputed that, in its provision of products and services, and in effecting the Data Transfers, Meta Ireland processes Users' personal data *qua* controller.

4.3 In its Response to the PDD, Meta Ireland notes that it "*is the provider of the Facebook service … and the controller of the processing of personal data for the purposes described in [Meta Ireland's] data policy … for users in the European region*".[20]

Personal Data

4.4 The 2018 DTPA identifies - in Appendix 1, Part A, to the 2010 SCCs outlined in Schedule 1 thereto - the nature and extent of the personal data of Users that is in fact the subject of the Data Transfers. This includes the following categories of personal data:

> *" … the personal data generated, shared and uploaded by or about individuals who visit, access, use or otherwise interact with the products and services of the data exporter (including Facebook and Instagram).*

[20] Response to the PDD, Part A, paragraph 1.1.

- *information related to the things users do and the information users provide when using the services (such as profile information, posted photos and videos, shared location information, communications between users, and related information about use of the products and services);*

- *information related to the data subjects that other users of the products and services provide (such as a user's imported contacts or photos);*

- *information related to users' networks and connections (such as a user's connections to groups, pages, and other users);*

- *information related to payments (such as information related to purchases or financial transactions);*

- *information about devices (such as information from or about the computers, phones or other devices where users install software provided by, or that access products and services of, the data exporter);*

- *information from websites and apps that use products and services of the data exporter (such as information about visits to third-party websites or apps that use a "like" or "comment" button or other service integrations); and*

- *information from third-party partners (such as information related to jointly offered services or use of third party services); and information from affiliates of Facebook and companies in the Facebook family of companies.*

Special categories of data

Such data may include:

- *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation; and*

- *genetic data and biometric data (as those terms are defined in the GDPR) for the purpose of uniquely identifying a natural person."*

4.5 The 2021 DTPA identifies the data transferred in similar terms.

Processing

4.6 In the Judgment, the CJEU held that the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) GDPR, carried out in a Member State, and that it falls within the scope of the GDPR under Article 2(1) thereof.[21]

4.7 There is no dispute that Meta Ireland makes the Data Transfers to Meta US. Meta Ireland notes in its Response to the PDD:

> "*At all material times to date, personal data of [Meta Ireland] Users controlled by [Meta Ireland]… has been and is transferred from the EU/EEA by [Meta Ireland] to its processor [Meta US], in the United States of America … for the purposes of providing the Facebook Service to [Meta Ireland] Users*".[22]

4.8 As such, the Data Transfers between Meta Ireland and Meta US clearly involve transfers of personal data to a third country, the US, giving rise to "*processing*" within the meaning of the GDPR, in accordance with the Judgment.

Cross-Border Processing

4.9 The concept of "*cross-border processing*" is defined in Article 4(23) GDPR as either:

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

[21] Judgment, paragraph 83.
[22] Response to the PDD, Part A, paragraph 1.3.

4.10 While it does not appear to be explicitly addressed in any one or more of the Response to the PDD, the Supplemental Response to the PDD, or the Response to the RPDD, it is not disputed that the processing at issue here is cross-border processing.

4.11 Meta Ireland has notified the DPC that Ireland is its place of main establishment in the EU.[23] Whilst the issue of Meta Ireland's *"main establishment"* is dealt with separately below, I find that the "*processing*" of personal data undertaken by Meta Ireland in connection with the Data Transfers is "*cross-border processing"* within the meaning of Article 4(23)(a) GDPR in circumstances where all such Meta US products and services as are provided to Users in the EU/EEA are provided by Meta Ireland, being a controller in the EU which, whilst understood to have a number of establishments within the EU, has its place of central administration in the EU in Ireland, where decisions on the purposes and means of the processing of Users' personal data are taken.

4.12 Alternatively, and if I am incorrect in my understanding that Meta Ireland has other establishments in the EU, it appears that the processing which Meta Ireland undertakes substantially affects or is likely to substantially affect data subjects in more than one Member State within the meaning of Article 4(23)(b) GDPR. In this regard, I note that in her Affidavit, Ms Cunnane averred that while, for those individuals based in the US and Canada, the Facebook Service is provided by Meta US, critically, "*for individuals in the rest of the world, including in the EU, the Facebook Service is provided by [Meta Ireland]*".[24] This indicates that the Facebook Service is provided to EU data subjects by Meta Ireland, and as such, processing undertaken in that context substantially affects or is likely to substantially affect data subjects in more than one Member State.

Lead Supervisory Authority

4.13 In circumstances where the Data Transfers involve cross-border processing of Users' personal data, it follows that the supervisory authority being competent to act as lead supervisory authority in respect of such processing for the purposes of Article 60 GDPR falls to be determined by reference to Article 56 GDPR. In that context, Article 56(1) GDPR provides that the supervisory authority *"of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-*

[23] By email dated 25 May 2018, from Yvonne Cunnane to the Commissioner, and others.
[24] Affidavit of Yvonne Cunnane sworn on 8 November 2016 in the High Court Proceedings, paragraphs 7–9.

border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

4.14 As noted above, Meta Ireland previously notified the DPC that it has its *"main establishment"* in Ireland.

4.15 "*Main establishment*" is defined at Article 4(16)(a) GDPR to mean, as regards a controller with establishments in more than one Member State:

> "*the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment"*.

4.16 It appears to be clear that Ireland is the place of Meta Ireland's "*central administration*" in the EU, where "*decisions on the purposes and means of the processing of personal data are taken*."

4.17 Quite apart from the fact that Meta Ireland itself has notified the DPC that Ireland is its place of main establishment in the EU, it is noted that, in the High Court Proceedings, Ms Cunnane averred that Meta Ireland is a limited liability company, established under Irish law, with its registered office and principal place of business in Dublin, and that it is part of the Meta group of companies.[25]

4.18 Ms Cunnane further averred that the "*Facebook Service*" is a popular social network service, provided via the website and platform *www.facebook.com*, as well as via applications for mobile telephones and other devices. As noted above, for those individuals based in the US and Canada, the Facebook Service is provided by Meta US. However, critically, "*for individuals in the rest of the world, including in the EU, the Facebook Service is provided by [Meta Ireland]*".[26]

[25] Affidavit of Yvonne Cunnane, sworn on 8 November 2016, paragraph 5.
[26] Affidavit of Yvonne Cunnane, paragraphs 7–9.

Summary

4.19 I find that in circumstances where Meta Ireland has its main establishment in Ireland, the DPC is competent to act as lead supervisory authority, within the meaning of Article 56(1) GDPR, in respect of the Data Transfers, the conduct of which constitutes cross-border processing.

4.20 This further means that the onus fell on the DPC to prepare the Draft Decision required pursuant to Article 60(3) GDPR in connection with the particular issues under consideration in the context of the within Inquiry.

5. LEGAL PROVISIONS REGULATING THE DATA TRANSFERS

5.1 All EU-US data transfers–including the Data Transfers–are regulated by a range of legal provisions.

Charter

5.2 Article 7 of the Charter states that everyone has the right to respect for his or her private and family life, home and communications.

5.3 Article 8(1) of the Charter confers on everyone the right to the protection of personal data concerning him or her.

5.4 Article 8(2) of the Charter provides that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. It provides that everyone has a right of access to data which has been collected concerning him or her and the right to have it rectified.

5.5 Meanwhile, Article 47 of the Charter provides that everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in Article 47 of the Charter. These include a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law.

5.6 Article 52 of the Charter recognises that the rights and freedoms recognised by the Charter may be limited, but any such limitation must be provided for by law and respect the essence

of those rights and freedoms. Subject to the principle of proportionality, the limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

GDPR

5.7 Article 44 GDPR provides as follows:

> *"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*

5.8 Article 45 GDPR makes provision for "*Transfers on the basis of an adequacy decision*".

5.9 Article 45(1) GDPR provides that a transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. It further provides that such a transfer "*shall not require any specific organisation*".

5.10 Article 45(2) GDPR provides that, when assessing the adequacy of the level of protection, the European Commission shall, in particular, take account of the following elements:

> "*(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;*

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

5.11 Article 45(3) GDPR provides that the European Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of Article 45(2) GDPR. As at the date of adoption of this Decision, no adequacy decision is in place in respect of the transfers of personal data from the EU/EEA to the United States.

5.12 Meanwhile, Article 46 GDPR deals with "*Transfers subject to appropriate safeguards*".

5.13 Article 46(1) GDPR provides that in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor "*has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*".

5.14 Article 46(2) GDPR provides that the "*appropriate safeguards*" may be provided for, without requiring any specific authorisation from a supervisory authority, by the following:

(1) A legally binding and enforceable instrument between public authorities or bodies (Article 46(2)(a));

(2) Binding corporate rules in accordance with Article 47 (Article 46(2)(b));

(3) Standard data protection clauses adopted by the European Commission in accordance with the examination procedure referred to in Article 93(2) (Article 46(2)(c));

(4) Standard data protection clauses adopted by a supervisory authority and approved by the European Commission pursuant to the examination procedure referred to in Article 93(2) (Article 46(2)(d));

(5) An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Article 46(2)(e)); or

(6) An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Article 46(2)(f)).

5.15 Meanwhile, Article 49(1) GDPR provides for "*Derogations for specific situations*", and states that in the absence of an adequacy decision pursuant to Article 45(3) GDPR or of "*appropriate safeguards*" pursuant to Article 46 GDPR, transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(1) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (Article 49(1)(a));

(2) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request (Article 49(1)(b));

(3) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (Article 49(1)(c));

(4) The transfer is necessary for important reasons of public interest (Article 49(1)(d));

(5) The transfer is necessary for the establishment, exercise or defence of legal claims (Article 49(1)(e));

(6) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent (Article 49(1)(f));

(7) The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case (Article 49(1)(g)).

5.16 Article 49(1) GDPR further provides that where a transfer could not be based on a provision in Article 45 or Article 46 GDPR, and none of the derogations for a specific situation in Article 49(1) GDPR is applicable, a transfer to a third country or an international organisation may take place only if:

(1) The transfer is not repetitive;

(2) The transfer concerns only a limited number of data subjects;

(3) The transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject;

(4) The controller has assessed all the circumstances surrounding the data transfer;

(5) The controller has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data;

(6) The controller has informed the supervisory authority of the transfer;

(7) The controller has, in addition to providing the information referred to in Articles 13 and 14, informed the data subject of the transfer and of the compelling legitimate interests pursued.

The SCC Decisions

5.17 As is clear from the provisions set out above, SCCs adopted by the European Commission comprise one method of providing "*appropriate safeguards*" in the absence of an adequacy decision pursuant to Article 46(2)(c) GDPR.

5.18 The 2010 SCC Decision was adopted pursuant to Article 26(4) of the Directive, and, pursuant to Article 46(5) GDPR, was stated to remain in effect until amended, replaced or repealed by a Commission Decision adopted in accordance with Article 46(2) GDPR.

5.19 The 2021 SCC Decision was adopted on 4 June 2021, repealing the 2010 SCC Decision with effect from 27 September 2021, and setting out new SCCs (the 2021 SCCs) which came into effect on 27 June 2021.

5.20 Having regard to the temporal scope of the Inquiry (and subject to what I say in Section 6 of this Decision), relevant provisions of both the 2010 SCC Decision and the 2021 SCC Decision are set out below.

The 2010 SCC Decision

5.21 Recital 11 of the 2010 SCC Decision reads as follows:

> "*Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject*."

5.22 Article 1 of the 2010 SCC Decision states:

"*The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive [95/46].*"

5.23 Article 2 of the 2010 SCC Decision provides that the 2010 SCC Decision "*shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as data processors*".

5.24 Article 3 of the 2010 SCC Decision provides that, for the purpose of the 2010 SCC Decision, the following definitions apply:

(1) "*data exporter*" means the controller who transfers the personal data (Article 3(a));

(2) "*data importer*" means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of the 2010 SCC Decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of the Directive (Article 3(b)); and

(3) "*applicable data protection law*" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established (Article 3(f)).

5.25 Article 4 of the 2010 SCC Decision–as amended by Implementing Decision 2016/2297–provides:

"*Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of [the Directive] leading to the suspension or definitive ban of data flows to third countries in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the [European] Commission which will forward the information to the other Member States.*"

The 2010 SCCs

5.26 The Annex to the 2010 SCC Decision, under the heading "*Standard Contractual Clauses (Processors)*", is comprised of 12 SCCs.

5.27 Clause 3, under the heading "*Third-party beneficiary clause*", provides in Clause 3(1) that:

> "*The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary*."

5.28 Omitted from the third-party beneficiary clause are Clauses 4(a), 4(j) and 5(f).

5.29 Clause 3(2) provides that:

> "*The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity*."

5.30 Clause 4 (a) provides that the data exporter agrees and warrants:

> "*that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State*".

5.31 Clause 4(j) provides that the data exporter warrants that it will ensure compliance with Clause 4(a)–(i).

5.32 Meanwhile, as the CJEU observed in the Judgment, it is clear from the 2010 SCCs (Clauses 4(a), 4(b), 5(a), 9 and 11(1)), that the data exporter and data importer confirm that they will comply with the applicable data protection law, namely, the GDPR, read in the light of the Charter.[27]

5.33 Clauses 5(a) and (b) confer on the data exporter the right to suspend the transfer and/or to terminate the contract, and the data exporter is obliged to suspend the data transfer and to terminate the contract where the data importer is not, or is no longer, able to comply with the 2010 SCCs.[28]

5.34 Thus, Clause 4(a) and Clause 5(a) and (b) oblige the data exporter and the data importer to satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the 2010 SCCs in the Annex to the 2010 SCC Decision, before transferring personal data to that third country.[29]

5.35 In particular, according to the footnote to Clause 5, the data exporter and data importer must consider whether or not "*mandatory requirements of [the third country's legislation] … go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security*". Compliance by the data importer with a mandatory requirement which goes beyond what is necessary for these purposes "*must be treated as a breach of those clauses*".[30]

5.36 The data importer is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.[31]

<u>The 2021 SCC Decision</u>

5.37 Also relevant are the 2021 SCC Decision and the 2021 SCCs. The DPC agrees with Meta Ireland's submissions regarding the relevance of these provisions.[32]

5.38 On 4 June 2021, the European Commission adopted Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries

[27] Judgment, paragraph 138.
[28] Judgment, paragraph 140.
[29] Judgment, paragraph 141.
[30] Judgment, paragraph 141.
[31] Judgment, paragraph 142.
[32] Response to the PDD, Part B, paragraphs 1.9 and 1.10; Part C, paragraph 3.9.

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**the 2021 SCC Decision**"), containing new standard contractual clauses in the Annex to the 2021 SCC Decision (including the clauses set out in Module Two), under Article 46(2)(c) GDPR ("**the 2021 SCCs**"). The 2021 SCCs came into effect on 27 June 2021.

5.39 As Meta Ireland observe,[33] the European Commission has noted that the 2021 SCCs,

> " … *reflect new requirements under the [GDPR] and take into account the [CJEU Judgment], ensuring a high level of data protection for citizens", "offer more legal predictability to European businesses … while allowing data to move freely across borders, without legal barriers"* and *"take into account the joint opinion of the [EDPB] and the European Data Protection Supervisor, feedback from stakeholders during a broad public consultation and the opinion of Member States' representatives*".[34]

5.40 Article 1(1) of the 2021 SCC Decision states as follows:

> *"The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer)."*

5.41 Article 2 provides that:

> *"Where the competent Member State authorities exercise corrective powers pursuant to Article 58 of Regulation (EU) 2016/679 in response to the data importer being or becoming subject to laws or practices in the third country of destination that prevent it from complying with the standard contractual clauses set out in the Annex, leading to the suspension or ban of data transfers to third countries, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States."*

[33] Response to the PDD, paragraph 1.9.
[34] "European Commission adopts new tools for safe exchanges of personal data", accessible at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2847 .

The 2021 SCCs

5.42 The 2021 SCCs – as set out in the Annex to the 2021 SCC Decision - contain 18 discrete clauses, with certain of the clauses in turn containing a series of "modules", with the precise content of each such module being adjusted to facilitate its application to the following categories of transfers, being controller to controller (Module 1); controller to processor (Module 2), processor to processor (Module 3) and processor to controller (Module 4).

5.43 Clause 1(a) sets out the purpose of the 2021 SCCs in the following terms:

> *"The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country."*

5.44 Clause 2 (headed "Effect and invariability of the Clauses") provides (at sub-paragraph (a)) that,

> *"These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix …"*

5.45 Clause 3 establishes a right in favour of data subjects to "invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer", subject to the exceptions listed therein.

5.46 At Clause 8 (headed "Data protection safeguards"), the data exporter warrants that *"it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses."* From there, the clause identifies the parties' respective obligations under a series of headings, to include headings referable to the principles relating to the processing of personal data as set out at Article 5 GDPR.

5.47 Under the heading "Local laws and practices affecting compliance with the Clauses", Clause 14 contains a series of detailed provisions – applicable across all four modules – laying down

specific procedural steps required of the exporting and importing parties in connection with data transfers, underpinned by a number of warranties and declarations. It provides as follows:

> *"(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.*
>
> *(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:*
>
> *(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;*
>
> *(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;*
>
> *(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.*
>
> *(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with*

relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply."

5.48 Clause 15 in turn identifies certain specific obligations to which the importing party is subject (across all four modules) "in case of access by public authorities". It provides as follows:

"15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request."

5.49 Clause 16 is headed "Non-compliance with the Clauses and termination" and provides as follows:

"(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal

data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679."

6. FACTUAL POSITION RELATING TO THE DATA TRANSFERS

6.1 Meta Ireland accepts that at the material times for the purpose of the Inquiry, it has made the Data Transfers pursuant to the 2010 SCCs and now pursuant to the 2021 SCCs.[35]

6.2 Meta Ireland has recently implemented the 2021 SCCs as evidenced by the 2021 DTPA.

The 2015 DTPA and the 2018 DTPA

6.3 I am also aware from evidence adduced by Meta Ireland during the High Court Proceedings that the Data Transfers were, at that time, subject to intra-group agreements between Meta Ireland and Meta US, being the 2015 DTPA and the 2018 DTPA.[36]

6.4 As Ms Cunnane averred of the 2015 DTPA, "*[t]he DTPA is based on the [2010] SCCs for the transfer of personal data to processors established in third countries*" approved by the European Commission in the 2010 SCC Decision, and which have already been outlined above.[37]

6.5 On 10 December 2018, Meta Ireland, through their solicitors, notified the DPC that Meta Ireland and Meta US had entered into the 2018 DTPA, effective from 25 May 2018. A copy of

[35] Response to the PDD, paragraph 1.3.
[36] Affidavit of Yvonne Cunnane, paragraph 57; Exhibit "**YC1**".
[37] Affidavit of Yvonne Cunnane, paragraph 14.

the 2018 DTPA was also made available to the DPC. I have reviewed both the 2015 DTPA and the 2018 DTPA (together referred to hereinafter as "**the Agreements**").

6.6 It is apparent that the 2018 DTPA (like the 2015 DTPA) served at least two distinct purposes. Firstly, and by reference to the requirements of Article 28(2) GDPR, it regulated such processing of personal data as was then being carried out by Meta US, as processor, for and on behalf of Meta Ireland, as controller. Secondly, and separately, it identified the legal basis upon which (and the transfer mechanism by which) identified categories of personal data, including but not limited to Users' personal data, were subject to the Data Transfers. In the latter regard, the 2018 DTPA recorded that transfers of Users' personal data were made under and by reference to the form of SCCs for which provision was made in the 2010 SCC Decision, being the particular form of 2010 SCCs developed for controller to processor transfers.[38]

6.7 It is not apparent to me that there were any material distinctions between the Agreements (or either of them) and the 2010 SCCs. In particular, and as noted above, it is apparent that the 2018 DTPA incorporated the particular form of the 2010 SCCs for which provision was made in the Annex to the 2010 SCC Decision.

2021 DTPA

6.8 On 31 August 2021, Meta Ireland entered into a new transfer and processing agreement with Meta US, being the 2021 DTPA. In broad terms, this agreement serves a similar purpose to the previous 2018 DTPA. Importantly, however, the agreement incorporates the 2021 SCCs pursuant to the 2021 SCCs Decision. That is to say, as and from 31 August 2021, the Data Transfers are grounded in the 2021 SCCs Decision and the 2021 SCCs.

Assessment under Clause 14 of the 2021 SCCs

6.9 On or before entering into the 2021 DTPA, Meta Ireland and Meta US undertook (and documented) the form of assessment called for at Clause 14(b) of the 2021 SCCs, a copy of which was provided to the DPC (in its finalised form) on 1 September 2021. That document (referred to by Meta Ireland as a "Transfers Impact Assessment", or "TIA") comprises the following elements:

[38] Note that, at paragraph 18 of her Affidavit sworn on 8 November 2016, Yvonne Cunnane averred that "[t]o the best of my knowledge and believe, Facebook Ireland does not transfer any Facebook Ireland User Data to Facebook Inc in reliance on the SCCs approved by the European commission in Decision 2001/497/EC or Decision 2004/915/EC."

(1) Transfer Impact Assessment – Summary.

(2) A "factors assessment".

At paragraph 1.6 of this document, Meta Ireland describes the purpose this particular assessment in the following terms:

> *"In the context of the assessment of relevant US law and practice and the documenting of measures and safeguards required by the CJEU Judgment and the 2021 SCCs, this paper sets out circumstances of the transfer of User Data from FIL to FB, Inc. that have been taken into account to inform the case-by-case assessment that FIL and FB, Inc. must make in accordance with the decision in the CJEU Judgment and the 2021 SCCs."*

(3) An "equivalence assessment".

At internal paragraph 1.3, the assessment (which is said to have been conducted between Meta Ireland and Meta US, and endorsed by their external legal advisors) is described in the following terms:

> *"This assessment (i) comprises a detailed examination of Relevant EU Law to determine the level of protection that is required to be afforded to data subjects by EU law to comply with Article 46 GDPR (the "EU Standard"); and (ii) takes into consideration the 2021 SCCs and the relevant aspects of the US legal system (including laws and practices) as regards any access by US public authorities to the personal data transferred. These relevant aspects are then assessed in light of the EU Standard to determine whether data subjects whose personal data are transferred to the US pursuant to the 2021 SCCs are afforded an adequate level of protection. [Meta Ireland's] conclusion as a result of this assessment is that the level of protection afforded by relevant US law and practice to data subjects whose personal data is transferred by [Meta Ireland] to [Meta US] in the US pursuant to the 2021 SCCs is essentially equivalent to that guaranteed by Relevant EU Law as reflected by the EU Standard. [Meta Ireland] will keep this assessment under review."*

(4) A "Record of Safeguards", i.e. record of the "measures and safeguards" deployed by Meta Ireland and/or Meta US "to comply with and supplement the measures

under the 2021 SCCs to further ensure that an adequate level of protection continues to apply to User Data transferred from [Meta Ireland] to [Meta US]. This table documents such organisational, technical, and legal measures and safeguards."

6.10 I will consider the 2021 DTPA below, along with the TIA. I will also have regard to Meta Ireland's Data Policy and Meta US's Transparency Report which demonstrate that Meta US complies with US law in respect of access requests.

Meta US's Compliance with US Law

6.11 It is clear that Meta US is subject to and acts in accordance with US law. Meta US's compliance with US law can be derived from (inter alia) Meta Ireland's Data Policy which notes that Meta Ireland may:

> *" … access, preserve and share your information with regulators, law enforcement or others:*
>
> *In response to a legal request, if we have a good-faith belief that the law requires us to do so. We can also respond to legal requests when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction and is consistent with internationally recognised standards."*

6.12 It is also apparent from the Affidavit of Ms Andrea Scheley in the High Court Proceedings that Meta US has a framework in place to review law enforcement requests for data and where it believes that the requests are inconsistent with applicable law and/or its policies, it can and does challenge those requests.

6.13 However, no evidence was adduced in the High Court Proceedings to suggest that Meta US would ever act contrary to US law and/or that it would ever refuse a request for access to Users' personal data that was lawful under US law.

6.14 I have also reviewed the Transparency Report, which provides information regarding Government Requests for User Data made to Meta US, and which includes statistical information regarding such requests. This information appears to be provided up to the second half of 2021. (I understand that such information is subject to a six-month reporting delay).

Summary

6.15 In summary, therefore, as a matter of fact, it appears that:

(1) Meta Ireland makes the Data Transfers pursuant to the 2021 SCCs and by reference to the assessments contained or comprised in the TIA;

(2) Meta US complies with US law, and this includes complying with access requests made by the US government when such access requests are made in accordance with US law.

7. LAWFULNESS OF THE DATA TRANSFERS

7.1 Turning to the lawfulness of the Data Transfers, a number of the findings in the Judgment are critical both in respect of the framework that I must adopt when assessing the lawfulness of the Data Transfers and in respect of the substance of that assessment itself.

Framework for the Assessment

7.2 Regarding the framework for the assessment, it is necessary to carefully scrutinise the Judgment. Meta Ireland suggests that the DPC's interpretation of the Judgment (as first reflected in the PDD and later restated in the RPDD) is "*incorrect in a number of important respects*".[39] This is not accepted.

7.3 ***First***, the Judgment makes clear[40] that, in the absence of an adequacy decision, transfers to a third country are permissible only if:

(1) The controller or processor has provided "*appropriate safeguards*";

(2) Data subjects have "*enforceable rights*"; and

(3) Data subjects have "*effective legal remedies*".

7.4 Clearly, this directly reflects the express terms of Article 46(1) GDPR, set out above.

[39] Response to the PDD, Part C, paragraph 1.1.
[40] Judgment, paragraphs 91 and 103.

7.5 ***Second***, while Article 46 GDPR does not specify the nature of the requirements flowing from the reference to "*appropriate safeguards*", "*enforceable rights*" and "*effective legal remedies*", regardless of which transfer mechanism is relied upon, a level of protection essentially equivalent to that which is guaranteed within the EU is required.[41]

7.6 ***Third***, the level of protection required must be assessed on the basis of the provisions of the GDPR, read in light of the fundamental rights enshrined in the Charter.[42]

7.7 ***Fourth***, if transfers are conducted under Article 46(1) GDPR, "*the appropriate safeguards*" to be implemented must compensate for any lack of data protection in the third country in order to ensure compliance with data protection requirements and data subjects' rights appropriate to processing within the EU.[43]

7.8 ***Fifth***, and following from this, when assessing whether there are appropriate safeguards, enforceable rights and effective legal remedies, it is necessary to consider both:

(1) The contractual clauses agreed between the controller or processor established in the EU and the recipient of the transfer established in the third country; and,

(2) As regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country.

7.9 As regards the latter, the factors to be taken into consideration in the context of Article 46 GDPR correspond to those set out, in a non-exhaustive manner, in Article 45(2) GDPR, set out above.[44]

7.10 ***Sixth***, as noted above, SCCs may comprise a particular form of "*appropriate safeguards*" for the purpose of data transfers to third countries.[45] This is envisaged by Article 46(2) GDPR also set out above.

7.11 ***Seventh***, however, as the CJEU found,[46] while SCCs are binding on a controller established in the EU and the transfer recipient in the third country, "*it is common ground that those clauses*

[41] Judgment, paragraphs 92–96.
[42] Judgment, paragraphs 101 and 105.
[43] Judgment, paragraphs 95 and 131.
[44] Judgment, paragraphs 104–105.
[45] Judgment, paragraph 91.
[46] Judgment, paragraph 125.

are not capable of binding the authorities of that third country, since they are not party to the contract".

7.12 Consequently, while there are situations in which, depending on the law and practices in force in the third country concerned, the transfer recipient is in a position to guarantee the necessary protection of the data solely on the basis of SCCs, there are others in which the content of the SCCs may not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned.[47]

7.13 Critically, in this respect, the CJEU held that:

> "*That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates*".[48]

7.14 ***Eighth***, if the SCCs fail to provide the required level of protection and to compensate for any lack of data protection in the third country, it will be necessary to consider whether there are any supplemental measures in place which could compensate for inadequate protection in the third country.

7.15 In this regard, the CJEU held that Article 46 GDPR does not require that "*all safeguards*" must necessarily be provided for in a Commission decision.[49]

7.16 Rather, "*…. it may prove necessary to supplement the guarantees contained in [the] standard data protection clauses*" by providing "*other clauses of additional safeguards*" to "*supplement*" the SCCs.[50]

7.17 Moreover, "*depending on the prevailing position in a particular third country*", "*supplementary measures*" may need to be adopted by the controller to ensure compliance with the level of protection available within the EU.[51]

7.18 Thus, the controller or processor must:

[47] Judgment, paragraph 126.
[48] Judgment, paragraph 126.
[49] Judgment, paragraph 128.
[50] Judgment, paragraph 132.
[51] Judgment, paragraph 133.

> " … *verify, on a case-by-case basis and, where appropriate, in collaboration with the [importer] whether the law of the third country … ensures adequate protection, under EU law … by providing, where necessary, additional safeguards to those offered by [the 2010 SCCs]*."[52]

7.19 ***Ninth***, where the controller or a processor established in the EU is not able to take adequate additional measures to guarantee the requisite protection, the controller or processor, or failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned.

7.20 Significantly, the CJEU added:

> "*That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union* ***obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access*** *by the public authorities of that third country to that data*".[53]

7.21 This last point is important. While Meta Ireland is correct to note that the CJEU did not invalidate the 2010 SCC Decision—and SCCs generally—"*despite the fact that SCCs cannot bind the public authorities of a third country*",[54] it is clear that the CJEU took the view that where public authorities in the third country have access to data, there is a particular risk that no adequate additional measures to guarantee the requisite protection can be taken and that the controller, processor or competent supervisory authority must suspend or end such data transfers. Indeed, Meta Ireland acknowledges this in its reference to paragraph 126 of the Judgment. However, as will be clear from its contents, referenced above, paragraph 135 of the Judgment goes further than paragraph 126 in identifying the risk that SCCs and supplementary measures will be inadequate where public authorities have access to data.

7.22 In summary, therefore, arising from these findings in the Judgment, I am satisfied that I must consider:

(1) Whether US law provides a level of protection that is essentially equivalent to that provided by the GDPR, read in light of the fundamental rights in the Charter;

---

[52] Judgment, paragraph 134.
[53] Judgment, paragraph 135. Emphasis added.
[54] Response to the PDD, Part C, paragraph 2.2(C).

(2) If not, whether the 2010 SCCs and/or the 2021 SCCs can compensate for any inadequacies in the protection afforded by US law; and

(3) If not, whether there are any supplemental measures in place which can compensate for any inadequacies in the protection afforded by US law.

7.23 While Meta Ireland seems to suggest that its interpretation of the assessment required by the Judgment differs from that identified by the DPC, in reality, that does not seem to be the case and Meta Ireland's approach appears to reflect the tripartite structure adopted by the DPC and just identified.[55]

Meta Ireland's Response on the Interpretation of the Judgment

7.24 It is apparent from its Response to the PDD that Meta Ireland takes issue with my interpretation of the Judgment in a number of respects. Whilst I engaged with those objections in the context of the RPDD and explained why I do not accept them, substantially the same objections were largely repeated in Meta Ireland's Response to the RPDD. (Certain of these objections are also referenced in the USG's Response to the RPDD).

7.25 ***First***, throughout the Response to the PDD, and largely repeated, albeit in summary form, in its Response to the RPDD, Meta Ireland seems to identify its own test for determining suitability of supplemental measures by lowering the standard to include measures that can "*address*" or "*mitigate*" any "*relevant remaining*" inadequacies in the protections offered by US law and practice and the SCCs.[56] In particular, Meta Ireland has suggested (in its Response to the PDD) that the second part of the assessment requires considering, if there is no essential equivalence:

> " … *whether the 2021 SCCs alone (including by reference to enforceable data subject rights and effective legal remedies available in the EU) sufficiently* ***address****, compensate for or* ***mitigate*** *any inadequacies in the protection afforded by US law and practice in respect of the [Meta Ireland] Data Transfers*".[57]

[55] Response to the PDD, Part C, paragraph 2.4.
[56] Response to the PDD, Part C, paragraphs 3.12, 4.2(C), 4.2(D), 4.3(B), 4.3(C) ; Part E, paragraphs 1.2, 6.1, 7.7 ; Part G, paragraph 2.10(C).
[57] Response to the PDD, Part C, paragraph 4.3(B). Emphasis added.

7.26 Similarly, it has suggested that the third part of the framework should be formulated in the following terms:

> "*If not, whether there are any supplemental measures in place relevant to the [Meta Ireland] Data Transfers which can* ***address****, compensate for or* ***mitigate*** *any relevant raining inadequacies in the protection afforded by both US law and practice and the 2021 SCCs (including by reference to enforceable data subject rights and effective legal remedies available in the EU)*".[58]

7.27 However, the terms "*mitigate*" and "*address*" cannot be found in either the Judgment or the GDPR.

7.28 By contrast, Recital (108) to the GDPR on transfers in the absence of an adequacy decision refers to the requirement for controllers and processors to take measures to "*compensate*" for the lack of data protection in a third country by way of appropriate safeguards. The DPC is therefore concerned that Meta Ireland is seeking to promote a lower standard for the objective of SCCs and supplemental measures than is permitted by the Judgment and the GDPR. The DPC is also concerned that this proposed standard ignores the essence of paragraphs 132 and 133 of the Judgment—to which reference has already been made above—which emphasise that one of the reasons that supplementary measures may be required is because of the fact that SCCs cannot provide guarantees beyond a contractual obligation and do not bind public authorities of third countries.

7.29 Accordingly, and taking account of Recital (108) to the GDPR, it is the DPC's view that the requirement on a controller is to take measures which "*compensate*" for the lack of data protection in the third country, and not those which alternatively "*address*" or "*mitigate*" the deficiencies.

7.30 ***Second***, it is notable that in its Responses to the PDD and the RPDD, respectively, Meta Ireland appears to seek to re-open a debate—which was considered at length in the High Court Proceedings and unequivocally resolved by the CJEU—in respect of whether a distinction must

[58] Response to the PDD, Part C, paragraph 4.3(C). Emphasis added.

be drawn between the operation of Articles 45 and 46 GDPR (and corresponding Recitals (104) and (108)).[59]

7.31 For example, Meta Ireland claims[60] that *"[t]he CJEU's consideration of US law was therefore in the context of Article 45 GDPR, not Article 46 GDPR. A different assessment is required under Article 46 GDPR*".

7.32 The DPC accepts Meta Ireland's submission[61] that in the context of Article 46 GDPR, the relevant protections do not need to be provided "***solely*** *by virtue of the laws and practices of the third country but can instead be provided in the EU* ***or*** *in the third country*".[62]

7.33 However, the DPC does not accept the submission that a "*different assessment*"—less still a "*materially different*" assessment[63]—is required under Articles 45 and 46 GDPR. The position of the CJEU was clear regarding the relationship between Articles 45 and 46 GDPR. In this regard also, the statement of the EDPB quoted by Meta Ireland[64] that "*[t]he reasons for the invalidation of the Privacy Shield [Decision] also have consequences on other transfer tools*" is entirely correct.

7.34 In particular, the Judgment is clear that, regardless of which part of Chapter V is used to underpin transfers, Article 44 GDPR requires "*essential equivalence*" of protection to be reached in each case,[65] to ensure that the level of protection guaranteed by the GDPR is not undermined.

7.35 The DPC is bound by these findings, and it is not open to the DPC to conclude that the CJEU's analysis was incorrect.

7.36 It is also the case that Meta Ireland's position ignores the fact that identical factual matrices—insofar as the State surveillance regime and the ability of US State authorities to request access to data—apply to transfers to the US regardless of the transfer mechanism at issue. In this regard, the CJEU's assessment of the nature and effect of US law with regard to the standards

[59] See, e.g., Part A, paragraphs 2.4(A) and 2.4(C); Part C, paragraphs 2.2(B), 2.4(A), 3.5(B), and 3.9; Part E, paragraphs 4.4, 4.10(A) and 5.18 of the Response to the PDD. See also, for example, paragraph 1.2 of the Response to the RPDD.
[60] Response to the PDD, Part A, paragraph 2.4(A)(1).
[61] Response to the PDD, Part B, paragraph 2.2(B).
[62] Meta Ireland's emphasis.
[63] Response to the PDD, Part C, paragraph 3.5(B)(1).
[64] Response to the PDD, Part E, paragraph 4.10(A).
[65] See, e.g., Judgment, paragraphs 94—96. See also paragraph 7.5 above.

required under EU law is equally applicable to data which was transferred to the US under the Privacy Shield as it now is to data currently being transferred pursuant to the 2021 SCCs.

7.37 It is also relevant to note here that, in the context of the Data Transfers, nothing turns on the fact that the form of assessment referenced at Article 46 GDPR calls for a consideration of the remedies available to Users within the EU as well as such remedies as may be available in the United States. In that regard, Meta Ireland fails to acknowledge that the particular remedies it says are available in the EU (and to which it is said regard must be had when conducting an assessment under Article 46 GDPR) are not such as would satisfy the requirements articulated at paragraph 187 of the Judgment. There, the CJEU recalled (by reference to its earlier judgment in Case C-362/14, *Schrems*), that *"legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."* On no assessment could it be said that any of the remedies available to Users within the EU (to include those listed at Part E, paragraph 4.29, of the Response to the PDD) is capable of providing an effective remedy, consistent with the requirements of paragraph 187 of the Judgment, where, for example, a US public authority accesses a User's data, post-transfer, without notice to the User, and in a manner incompatible with the requirements of EU law.

7.38 This reality was recognised by the CJEU at paragraph 189 of the Judgment where it noted that,

> *" … [t]he existence of such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on alleged unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third county."*

7.39 Accordingly, Meta Ireland is incorrect when it says (as it says at Part B, paragraphs 1.5 through 1.7 of its Response to the RPDD) that "[t]he DPC has failed to appreciate or engage with the difference in the nature of the assessment to be carried out under Articles 45 and 46 GDPR". The true position is Meta Ireland's contentions to the effect that, in the context of the Data

Transfers, there is some material difference between the assessments called for by Articles 45 and 46 GRPR, is not sustainable.

7.40 ***Third***, in its Response to the PDD, and again in its Response to the RPDD, Meta Ireland engages in an extensive discussion of various data retention and other CJEU and ECtHR cases.[66] However, having carefully considered the submissions made by or on behalf of Meta Ireland, I am satisfied that Meta Ireland's discussion of this case law does not undermine the DPC's analysis of the Judgment and the standards required. The DPC does not therefore regard it as necessary to respond in detail to this case law.

7.41 In particular, in this regard, in Part D of the Response to the PDD, Meta Ireland engages in an extensive discussion of the fundamental rights and freedoms engaged by its services. For the reasons discussed in Sections 8 and 9 below, however, the DPC does not accept that the rights and freedoms engaged are of relevance to its assessment of the first question under consideration in this particular Inquiry, namely, whether Meta Ireland is acting lawfully, and in particular, compatibly with Article 46(1) GDPR, in making the Data Transfers. As such, I do not consider the engaged rights and freedoms further for the purpose of this part of my analysis.

7.42 ***Fourth***, and more generally, regarding the ECtHR case law on which Meta Ireland relies, it is clear from paragraphs 98 and 99 of the Judgment that the ECHR does not constitute – as long as the EU has not acceded to it – a legal instrument formally incorporated into EU law. Therefore as already set out above,[67] the interpretation of EU law must be undertaken in light of the fundamental rights guaranteed by the Charter, not the ECHR.

7.43 It is of course accepted that the CJEU stated in *La Quadrature du Net* that Article 52(3) of the Charter "*is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union. Account must therefore be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection*".[68]

7.44 However, ultimately, the relevant standard to be applied is that of the Charter.

[66] Response to the PDD, Part E, paragraph 4.11.
[67] See paragraph 7.5.
[68] *La Quadrature du Net*, paragraph 124.

7.45 ***Fifth***, it is notable that, in the Response to the PDD, Part E, in which Meta Ireland undertakes its consideration of the Data Transfers, Meta Ireland does not follow the framework of assessment identified by the CJEU. At times, this has rendered it difficult to consider Meta Ireland's submissions, given that it is not always clear to which particular aspect of the assessment the relevant submission is addressed. However, in the discussion below, I have had full regard to Meta Ireland's submissions (to include those received in response to the RPDD) and have sought to address them in accordance with my views on their relevance to each of the elements of the assessment.

Whether US Law Provides an Essentially Equivalent Level of Protection

7.46 I now turn to the first part of the inquiry required by the Judgment, namely, whether US law provides an essentially equivalent level of protection.

7.47 In this regard, the Judgment makes a number of findings that are binding on me in my assessment.

7.48 In particular, it is apparent from the Judgment that US law does not–in itself–provide an essentially equivalent level of protection to that provided by the GDPR, read in light of Articles 7, 8 and 47 of the Charter.

7.49 This position was underpinned by the findings of fact as to US law made in the High Court Judgment (endorsed by the Supreme Court and accepted by the CJEU) and made by the European Commission in Commission Implementing Decision (EU) 2016/1250 ("**the Privacy Shield Decision**").[69]

Aspects of US Law Considered in the Judgment

7.50 A number of particular aspects of US law were relied on by the CJEU in the Judgment. (Whilst noting the USG's contention made at paragraph 7.4 of its Response to the RPDD - to the effect that the DPC is not bound by findings of fact made by the CJEU, to include findings in relation to matters of US law which are properly to be treated as being concerned with issues of fact - the critical point is that neither Meta Ireland nor the USG has pointed to any such factual

[69] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield ([2016] OJ L207/1).

matter, the import of which would be to displace any of the key findings made by the CJEU, details of which are set out in more detail below).

7.51 The US authorities' intelligence activities concerning the personal data transferred to the US are based, *inter alia*, on Section 702 FISA and on EO 12333. [70]

7.52 Section 702 FISA permits the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not US citizens located outside the US in order to obtain *"foreign intelligence information",* and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes.[71]

7.53 In the context of the PRISM programme, Internet service providers are required to supply the NSA with all communications to and from a "*selector*", some of which are also transmitted to the Federal Bureau of Investigation and the Central Intelligence Agency.[72]

7.54 As regards the UPSTREAM programme, telecommunications undertakings operating the *"backbone"* of the Internet–that is to say, the network of cables, switches and routers–are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a "*selector*". Under that programme, the NSA has access both to the Meta US data and to the content of the communications concerned.[73]

7.55 EO 12333 allows the NSA to access data "*in transit*" to the US, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. Activities conducted pursuant to EO 12333 are not governed by statute.[74]

Assessment–Articles 7 and 8 of the Charter

7.56 With respect to Articles 7 and 8 of the Charter, the CJEU observed that:

> "*access to a natural person's personal data with a view to its retention or use affects the fundamental right to respect for private life guaranteed in Article 7 … Such*

[70] Judgment, paragraph 60; High Court Judgment, paragraph 167.
[71] Judgment, paragraph 61; High Court Judgment, paragraph 168.
[72] Judgment, paragraph 61; High Court Judgment, paragraph 179.
[73] Judgment, paragraph 62; High Court Judgment, paragraphs 180–181; see also paragraph 182.
[74] Judgment, paragraph 63; High Court Judgment, paragraphs 175–176.

processing … also falls within the scope of Article 8 …and accordingly must necessarily satisfy the data protection requirements laid down in that article ….".[75]

7.57 It also observed that:

" *… the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference …*".[76]

7.58 While Articles 7 and 8 of the Charter are not absolute,[77] any limitation must be provided for by law and respect the essence of those rights and freedoms and, subject to the principle of proportionality, limitations may be made to those rights only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedom of others.[78]

7.59 The CJEU referred to the fact that, as regards the surveillance programmes based on Section 702 FISA, the European Commission found, in Recital (109) of the Privacy Shield Decision that, according to Section 702 FISA, "*the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)*".[79]

7.60 The CJEU further found that it was clear from Recital (109) of the Privacy Shield Decision that the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether "*individuals are properly targeted to acquire foreign intelligence information*".[80]

[75] Judgment, paragraph 170.
[76] Judgment, paragraph 171.
[77] Judgment, paragraph 172.
[78] Judgment, paragraphs 174–176.
[79] Judgment, paragraph 179.
[80] Judgment, paragraph 179.

7.61 Crucially, the CJEU found that:

> "*Section 702 … FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances … that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter … according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards*."[81]

7.62 Regarding the requirement for enforceable rights, the CJEU observed that, according to the findings in the Privacy Shield Decision, the implementation of the surveillance programmes based on Section 702 FISA is subject to the requirements of Presidential Policy Direction-28 ("**PPD-28**"). However, although the European Commission stated, in Recitals (69) and (77) of the Privacy Shield Decision, that such requirements are binding on the US intelligence authorities, the US Government accepted, in reply to a question put by the CJEU, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities.[82]

7.63 The CJEU further found that "*… [a]s regards the monitoring programmes based on E.O. 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either*."[83]

7.64 The CJEU added that PPD-28, with which the application of the PRISM and UPSTREAM must comply, allows for "'*bulk' collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection*", as stated in a letter from the Office of the Director of National Intelligence to the US Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision.

---

[81] Judgment, paragraph 180.
[82] Judgment, paragraph 181; see also High Court Judgment, paragraph 176 (noting that "*[t]here is no legal remedy for any actions of NSA pursuant to EO 12333*").
[83] Judgment, paragraph 182.

7.65 That possibility, which allows, in the context of the surveillance programmes based on EO 12333, access to data in transit to the US without that access being subject to any judicial review, does not delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.[84]

7.66 Consequently, the CJEU concluded that neither Section 702 FISA nor EO 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.[85]

7.67 It also held that the limitations on the protection of personal data arising from the domestic law of the US on the access and use by US public authorities of data transferred to the EU "*are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter*".[86]

Assessment–Article 47 of the Charter

7.68 Regarding Article 47 of the Charter, as already set out and as the CJEU held, this provision requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. Article 47 of the Charter provides that everyone is entitled to a hearing by an independent and impartial tribunal.[87]

7.69 The CJEU held that the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[88]

7.70 As the CJEU observed, the European Commission had found in Recital (115) of the Privacy Shield Decision, that:

[84] Judgment, paragraph 183.
[85] Judgment, paragraph 184.
[86] Judgment, paragraph 185.
[87] Judgment, paragraph 186.
[88] Judgment, paragraph 187.

> " … *while individuals, including EU data subjects, … have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered*".[89]

7.71 Thus, as regards EO 12333, the European Commission emphasised, in Recital (115) to the Privacy Shield Decision, the lack of any redress mechanism.

7.72 The CJEU therefore held that the existence of such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that presidential decree made it impossible to conclude that US law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

7.73 The CJEU reiterated that, as regards both the surveillance programmes based on Section 702 FISA and those based on EO 12333, neither PPD-28 nor EO 12333 grants data subjects rights actionable in the courts against the US authorities. From this, it followed that *"data subjects have no right to an effective remedy."*[90]

Aspects of US Law Relevant for Present Purposes

7.74 In the Judgment, the CJEU had regard to Section 702 FISA, including the PRISM programme, Section 702 FISA UPSTREAM, and EO 12333 in considering whether US law provides essentially equivalent protection for data subjects to that provided under EU law. I will consider these in turn.

Section 702 FISA PRISM

7.75 Section 702 FISA applies to both the UPSTREAM and PRISM programmes. Whilst reserving the DPC's position on the CJEU's engagement with, and treatment of, Section 702 FISA UPSTREAM and EO 12333, for the purpose of this section of the Decision, I focus on the PRISM programme under Section 702 FISA ("**PRISM**").

7.76 The Judgment is clear that, in a number of respects, PRISM results in US law not providing a standard of protection that is essentially equivalent to that provided by the GDPR, read in light

[89] Judgment, paragraph 191.
[90] Judgment, paragraph 192.

of Articles 7, 8 and 47 of the Charter. In this regard, the DPC places particular reliance on paragraphs 180, 184, 185 and 192 of the Judgment, as referred to above.

7.77 In addition, I am satisfied that PRISM does not satisfy the requirements of Article 52(1) of the Charter.

7.78 ***First***, Section 702 FISA fails to fulfil the requirement in Article 52(1) of the Charter that "*[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter* ***must be provided for by law***".[91]

7.79 Section 702 FISA limits Charter rights without such limitations being provided for by law, given that the legal basis permitting the interference does not define the scope of the limitation on the exercise of the right concerned. This can be derived from paragraphs 179 and 180 of the Judgment to the effect that Section 702 FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence.

7.80 Paragraph 183 of the Judgment is also relevant in this regard, with the CJEU noting:

> "*PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply [Section 702 FISA and EO 12333] allows for 'bulk' collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data*".

7.81 ***Second***, Section 702 FISA does not satisfy the requirement in Article 52(1) of the Charter that any limitations on Charter rights must be "*necessary*", i.e. the legislation providing for the interference must impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to effectively protect their personal data against the

[91] Emphasis added.

risk of abuse. In this regard, it is significant that the CJEU found (at paragraph 180 of the Judgment) that "*Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes*".

7.82 Overall, therefore, even limiting my focus for present purposes to PRISM, it is apparent that the standard of protection secured by US law is not essentially equivalent to that conferred by EU law. I am satisfied that nothing in the Responses to the PDD and RPDD received from Meta Ireland and the USG, respectively, changes that.

Section 702 FISA UPSTREAM

7.83 As discussed above, Section 702 FISA UPSTREAM applies to data in transit. I note that Meta Ireland has asked the DPC not to have regard to Section 702 FISA UPSTREAM, on the basis that Users' data is protected from collection pursuant to Section 702 FISA UPSTREAM requests.[92]

7.84 While I have noted the comments of the CJEU on Section 702 FISA UPSTREAM, on the basis of the conclusions I have reached in relation to PRISM, in my view it is not necessary for me to consider Section 702 UPSTREAM for the purposes of this Decision. However, that is not to say that I agree with Meta Ireland when it says that that there is no need to have regard to Section 702 FISA UPSTREAM simply by virtue of the measures Meta has imposed in order to protect Users' data from collection to include (most notably), encryption. For present purposes, however, I am satisfied that there is no need for me to interrogate those measures given the view I have reached in relation to PRISM.

EO 12333

7.85 Meta Ireland has also submitted that the DPC should not have regard to EO 12333, on the basis that this Executive Order is "*not relevant to the assessment the [*DPC*] is required to carry out in the context of the [Meta Ireland] Data Transfers in the Inquiry*".[93] Meta Ireland contends that this is because the Data Transfers are end-to-end encrypted in transit and EO 12333 does not provide the USG with legal authority to compel providers such as Meta Ireland to produce data or decryption keys.

[92] Response to the PDD, Part E, paragraph 4.6(A).
[93] Response to the PDD, Part E, paragraph 4.6(B). See also Part C, paragraph 2.3.

7.86 While I have noted the CJEU's comments on EO 12333 above, it is not necessary for me to consider EO 12333 or the reliability of the end-to-end encryption in my analysis in light of the conclusions I have reached in relation to PRISM. As noted above, my position on the CJEU's engagement with, and treatment of EO 12,333 (and UPSTREAM COLLECTION) is reserved.

Recent Developments in the Law of the EU and the US

7.87 One criticism made by Meta Ireland in its Response to the PDD (repeated in its Response to the RPDD) is that the DPC failed to take account of recent developments in US and EU law since the date of the Judgment.[94]

7.88 This criticism (which, contrary to what is contended for in Meta Ireland's Response to the RPDD, was in fact engaged with by the DPC in some detail in the RPDD), is not accepted. While the view of the DPC is that the detailed assessment of the CJEU in the Judgment that US law is not essentially equivalent to EU law is binding on it, the DPC is obviously willing to have regard to both developments in EU and US law that post-date the Judgment.

Recent Developments in the Law of the EU

7.89 With respect to developments in EU law, Meta Ireland refers to two cases: *La Quadrature du Net*[95] and *Privacy International*.[96]

7.90 Meta Ireland also relies on the discussion of these judgments in the EDPB Essential Guarantees Recommendations. However, Meta Ireland's citation from the EDPB Essential Guarantees Recommendations is incomplete and fails to acknowledge that the EDPB does not regard these judgments as affecting the analysis in the Judgment in Case C-362/14 or in the Judgment. Not only this, but it is clear from the discussion in the EDPB Essential Guarantees Recommendations that the EDPB regards the analysis in the Judgment in Case C-362/14 and the Judgment as remaining good law. This position is apparent from the following paragraphs that follow the section cited by Meta Ireland in the Response to the PDD (internal footnotes removed):

> "*35. In this regard, according to the settled case-law of the Court, derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In order to satisfy this requirement, besides*

[94] See, e.g., Response to the PDD, Part A, paragraph 2.4(C).
[95] Case C-511/18 *La Quadrature du Net v Premier Ministre* EU:C:2020:791.
[96] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* EU:C:2020:790.

laying down clear and precise rules governing the scope and application of the measure in question, the legislation in question must impose minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. "It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing".

36. ***In Schrems II, the CJEU has stressed that legislation of a third country which does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter****. Indeed, according to the case law, a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality,* ***itself define the scope of the limitation on the exercise of the right concerned.***

37. *Regarding the principle of necessity, the CJEU has made clear that legislations "authorising, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union (...) without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to the data and its use entail", do not comply with that principle. In* ***particular, laws permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.***

38. *Likewise, however this time when assessing a Member State law and not a third country law, the CJEU held in La Quadrature du Net and others, that "legislation requiring the retention of personal data* ***must always meet***

> ***objective criteria that establish a connection between the data retained and the objective pursued****". In the same context, in Privacy International, it also held that the legislator "must rely on objective criteria in* ***order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue***".

7.91 Thus, it is clear from the EDPB Essential Guarantees Recommendations that *La Quadrature du Net* and *Privacy International* are not to be regarded as qualifying or undermining the analysis in the Judgment.

7.92 I agree with this view, and a number of comments are worth making in this regard.

7.93 ***First***, it is accepted, as is pointed out in the EDPB Essential Guarantees Recommendations, in *La Quadrature du Net*, the CJEU ruled that the objective of safeguarding national security is, due to its importance, capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by other objectives such as of combatting crime.[97] However, it is very clear from the analysis and holdings in *La Quadrature* that processing to achieve national security objectives is nonetheless subject to significant restrictions.

7.94 ***Second***, in *La Quadrature du Net*, the CJEU confirmed that legislative measures which provide, ***as a preventive measure***, for the ***general and indiscriminate retention*** of traffic and location data, are precluded by the Directive on privacy and electronic communication, read in light of the Charter.[98] It follows from this that general and indiscriminate processing cannot be justified for preventive purposes. However, it is clear that PRISM is operated for preventative purposes. As set out above, Section 702 FISA permits the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not US citizens located outside the US in order to obtain "*foreign intelligence information*"; it is clearly capable of operating for preventive purposes.

7.95 ***Third***, the CJEU held (paragraph 168) that a number of measures for retention of data ***could*** be adopted for safeguarding national security, subject to a number of ***general preconditions***, namely, that the measures "*ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions*

[97] Paragraph 136.
[98] *La Quadrature du Net*, paragraph 168.

and that the persons concerned have effective safeguards against the risks of abuse". Yet the CJEU has already held that Section 702 FISA does not satisfy these general preconditions. In this regard, the CJEU found that Section 702 FISA "*does not indicate any limitations on the power it confers*" and that as a legal basis it did not itself "*define the scope of the limitation on the exercise of the right concerned*" or "*lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards*".

7.96 ***Fourth***, the CJEU found that provision could be made, for the purpose of safeguarding national security, for the targeted retention of traffic and location data, limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, "*for a period that is limited in time to what is strictly necessary, but which may be extended*". However, in the Judgment, the CJEU did not find that Section 702 FISA operated on such a targeted basis; rather, the CJEU concluded that Section 702 FISA "*does not indicate any limitations on the power it confers*".

7.97 ***Fifth***, the CJEU found (paragraph 168) that general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period "*limited in time to what is strictly necessary*" could be justified "*for the purposes of safeguarding national security*". Again, this is not the basis on which Section 702 FISA operates, as found by the CJEU in the Judgment.

7.98 ***Sixth***, the CJEU held that for the purpose of safeguarding national security, a Member State could have "*recourse to an instruction requiring providers of electronic communications services, **by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time**, the expedited retention of traffic and location data in the possession of those service providers*". For reasons already set out above, PRISM does not satisfy these requirements.

7.99 Consequently, I do not accept that *La Quadrature* affects the analysis in the Judgment.

7.100 Turning then to *Privacy International*, at issue was whether Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, was to be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.[99] The CJEU held (paragraphs 77—78) in relation to

[99] *Privacy International*, paragraph 50.

access to personal data provided under a Member State law, that "*general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary*".

7.101 The CJEU observed as follows:

> "*63. However, the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited).*
>
> *64. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*
>
> *65. It should be added that the requirement that any limitation on the exercise of fundamental rights* ***must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned*** *(judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).*"

7.102 At paragraph 67, the CJEU noted as follows:

> "*In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (see, to that effect, judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010, Volker und Markus Schecke*

and Eifert, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 76, 77 and 86; and of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 140)."

7.103 The CJEU added (at paragraph 68) that:

> *"In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, in particular where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016, Tele2, C-203/15 and C-698/15, EU:C:2016:970, paragraph 117; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 141*)."

7.104 While, as Meta Ireland notes[100], the CJEU accepted that the objective of safeguarding national security is capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by other objectives (paragraph 75), the CJEU added (at paragraph 76) that:

> "*…, in order to satisfy the requirement of proportionality referred to in paragraph 67 above, according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, national legislation entailing interference with the fundamental rights enshrined in Articles 7 and 8 of*

[100] Response to the PDD, Part E, paragraph 4.14.

the Charter ***must meet the requirements stemming from the case-law cited in paragraphs 65, 67 and 68 above***."

7.105 However, it is clear that PRISM does not satisfy these requirements. As already set out above, the CJEU concluded that Section 702 FISA "*does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence*".

7.106 As such, *Privacy International* does not assist Meta Ireland's position or suggest that the standards of EU law have been lowered since the Judgment such as to require a revisiting of the CJEU's assessment of US law.

Developments in US Law

Submissions made by Meta Ireland

7.107 In its TIA and, in particular, its "Essential Equivalence Assessment of Relevant US Laws and Practice", Meta Ireland submits that US law provides an essentially equivalent level of protection to EU data subjects whose personal data is transferred to the US under the 2021 DTPA.

7.108 In support of that proposition, Meta Ireland makes reference to certain developments in US law that post-date the Judgment (or, at least, post-date the hearing conducted before the CJEU) and which are said to bear on its essential equivalence analysis. The developments to which reference is made in this connection include (i) changes to the scope of Section 702 FISA as it operates in practice; (ii) a requirement that the USG memorialise a reasoned, written targeting determination for each individual targeted; and (iii) certain changes in privacy enforcement in the US.

7.109 Having carefully considered the positions contended for, I find these changes fail to remedy the particular gaps or deficiencies in US law, as identified by the CJEU in the Judgment. In particular, and by way of example, I note that they do not address the finding at paragraph 180 of the Judgment that Section 702 FISA does not indicate any limitations on the power it confers to implement surveillance programmes. Nor do they address (much less remedy) the fact that data subjects do not have the possibility of bringing a legal action in the United States before an independent and impartial court, in violation of Article 47 of the Charter.

7.110 It follows that, to the extent that Meta Ireland's TIA contends that US law has been the subject of changes post-dating the Judgment, such that US law can now be considered to provide essentially equivalent protection for data subjects to that provided under EU law, I disagree.

Submissions made by the USG

7.111 In its submissions in response to the PDD (dated 20 September 2021), the USG outlined certain developments in US law postdating the date of the hearing before the CJEU in Case C-311/18 (9 July 2019). In particular, it referenced:

- targeting procedures approved by the FISC dated 19 October 2020, which define how the government determines which specific persons' communications may be acquired, and which are said to be binding on the USG.
- assessments of compliance with Procedures and Guidelines issued pursuant to Section 702 of the FISA. (These assessments relate to periods that predated 9 July 2019 but were only authorised for public release on 2 April 2021 and 10 August 2021, respectively).
- Memorandum Opinions and Orders, from 6 December 2019 and 18 November 2020, respectively, in which the FISC granted approval of the certifications and related procedures regarding FISA 702 targeting procedures.
- Annual Statistical Transparency Reports for the years 2019 and 2020, which the Office of the Director of National Intelligence is required by statute to publish.
- FISC-approved NSA Section 702 Querying Procedures dated 19 October 2020.
- Judgments arising in *Wikimedia Foundation v. National Security Agency*[101].

7.112 Whilst noting these matters, I am satisfied that they, likewise, do not address the particular deficiencies in US law as identified by the CJEU at paragraphs 179 through 197 of the Judgment and, as such, they do not undermine the conclusions I have reached in relation to US law, as set out above. Noting that, in its subsequent Response to the RPDD, the USG complains that the DPC has failed to engage with the points referenced above, I repeat that the critical point

[101] Wikimedia Foundation v. National Security 857 F.3d 193 (4th Cir. 2017); Wikimedia Foundation v. National Security Agency, 427 F. Supp. 3d 582 (2019); Wikimedia Foundation v. National Security Agency, No. 20-1191 (4th Cir. Sept. 15, 2021).

here, in my view, is that none of the matters to which reference is made would operate to displace any of the key findings made by the CJEU, details of which have been set out above. This is not to dismiss the matters to which reference has been made by the USG, summarily or otherwise. Rather, it simply acknowledges that the gaps or deficiencies in US law as identified by the CJEU in the Judgment are not remedied by the matters to which reference is now made. In that regard, I also note, again, that none of the developments cited by the USG addresses the fact that, contrary to the requirements of Article 47 of the Charter, data subjects do not have the possibility of bringing a legal action in the United States before an independent and impartial court.

7.113 In truth, I believe it is clear that the USG's objections are targeted at the underlying findings made by the CJEU, to include, by way of example, that contained at paragraph 180 of the Judgment, described in the USG's Response to the RPDD as containing a *"sweeping and unfounded generalisation"* insofar as it expresses the CJEU's view that *"Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes."* Whilst respecting the fact that the USG disagrees with that assessment (the application of which it appears it would wish to see restricted), neither the matters cited at paragraph 7.111 above, nor those canvassed in the USG's Response to the RPDD, are such as would provide a basis on which the DPC could look behind the CJEU's conclusion-also contained in paragraph 180 of the Judgment-that *"[Section 702, FISA] cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter … according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself defined the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards."*

7.114 It is also relevant to note here that, contrary to what has been contended for by the USG in its Response to the RPDD, the fact that particular elements of the CJEU's analysis were undertaken by reference to the Privacy Shield does not detract from the general application of the CJEU's findings, not least where (taking paragraph 180 of the Judgment as a single example) the CJEU engaged with the relevant underlying provisions of US law directly.

Additional Meta Ireland Submissions

7.115 In the Response to the PDD (and again in its Response to the RPDD), Meta Ireland has also challenged my reliance on the findings in the Judgment regarding US law in a number of respects.

7.116 ***First***, Meta Ireland challenges the DPC's reliance on the CJEU analysis of relevant US law and practices on the basis that the CJEU did not rule on US law specifically in the context of Meta Ireland's data transfers.[102]

7.117 However, the DPC has never suggested that the CJEU ruled on US law specifically in relation to the Data Transfers.

7.118 Rather, the CJEU has said that "*essential equivalence*" must be achieved, whether by means of Articles 45 or 46 GDPR. The starting point of the assessment is, as explained above, an assessment of the third country laws and practices. This assessment was undertaken by the CJEU in the Judgment and the DPC is bound by the findings made by the CJEU in the course of the Judgment. The DPC also relies in this regard on the statement of the European Data Protection Board to which Meta Ireland itself refers that "*[t]he reasons for the invalidation of the Privacy Shield [Decision] also have consequences on other transfer tools*".[103]

7.119 Moreover, Meta Ireland complains that the CJEU's findings regarding inadequacies of US law generally in respect of personal data transferred from the EU to the US under the Privacy Shield Decision "*focusing in particular on the general application of Section 702 FISA and EO 12333, do not relate specifically to the [Meta Ireland] Data Transfers or consider how relevant US law and practice may in fact impact on the [Meta Ireland] Data Transfers*".[104] However, this statement is not understood given that Meta Ireland accepts that PRISM applies to its activities, and given that the DPC is obviously bound by the findings of the CJEU on Section 702 FISA.

7.120 ***Second***, at times, Meta Ireland's submissions in the Response to the PDD, in particular, appear to suggest that the DPC should simply ignore the findings in the Judgment.

7.121 For example, Meta Ireland suggests that there is an equivalence of EU remedies in the US.[105]

---

[102] See, e.g., Response to the PDD Part C, paragraphs 3.5(A), 3.8; Part E, paragraphs 4.1, 4.3, 4.26; Part G, paragraph 2.10(B).
[103] Response to the PDD, Part E, paragraph 4.10.
[104] Response to the PDD, Part C, paragraph 3.5(A).
[105] Response to the PDD, Part E, paragraph 4.29 and paragraphs 5.17—5.18.

7.122 However, this seems to suggest that what is required is a re-examination of the remedies available under US law by reference to the totality of those available in the EU, which cannot be correct.

7.123 This also ignores paragraphs 181, 182 and 192 of the Judgment, with the CJEU observing at paragraph 192 that:

> "*neither PPD28 nor EO12333 grants data subjects rights actionable in the Courts against the US authorities, from which it follows that data subjects have no rights to an effective remedy*".

7.124 ***Third***, Meta Ireland suggests that the DPC has placed undue emphasis on the perceived deficiencies in US law without having regard to the specific factual circumstances of the Data Transfers and the extent to which there is interference with Users' rights in practice in the US.[106] However, this is not accepted. The first part of the framework of analysis requires consideration of whether there is "*essential equivalence*" between the laws of the third country and those of the EU.

7.125 It is accepted that at paragraph 126 of the Judgment, the CJEU referred to the possibility of there being situations in which "*depending on the law and practice in force in the third country concerned*", the recipient of the data transfer may be in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses.

7.126 However, the focus of the CJEU was on the level of protection provided by reference to the ***law*** of the third country. For example, at paragraph 133 of the Judgment, the CJEU noted that the assessment had to take into consideration both the contractual clauses agreed and, as regards access by the public authorities of that third country to the personal data transferred, "*the relevant aspects of the **legal system** of that third country*".

7.127 In any event, even if there is a requirement to assess "*essential equivalence*" by reference to the ***practice*** of the third country, it is not accepted that Meta Ireland has demonstrated that ***practice*** in the US is such as to address the deficiencies identified above in the ***laws*** of the US.

7.128 ***Fourth***, Meta Ireland suggests that Section 702 FISA does not result in "*bulk*" collection. For example, Meta Ireland asserts that: "*in Meta US Inc's relevant and documented practical experience, requests from USG agencies in the national security context (which is the focus of*

[106] Response to the PDD, Part A, paragraph 2.4(C); Part E, paragraph 4.5.

the CJEU Judgment) do not amount to anything that could be considered 'bulk surveillance' but, on the contrary, are limited in nature to what is necessary and proportionate".[107]

7.129 However, regardless of whether Section 702 FISA is characterised as involving "*bulk surveillance*" or not, I am bound by the findings of the CJEU on Section 702 FISA, as already set out above.

7.130 In particular, I am bound by the finding of the CJEU at paragraph 180 of the Judgment that:

> "*It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.*"

7.131 It is also noted that it is not possible on the basis of the collated data Meta Ireland has provided[108] to assess the figures for total requests against affected accounts to be able to assess their claim of no bulk collection.

7.132 In any case, the fact remains that there is no dispute that Meta Ireland remains susceptible to bulk collection.

7.133 ***Fifth***, Meta Ireland suggests that I must consider whether US law offers essential equivalence, not by reference to the findings in the Judgment, but rather by reference to "*all the circumstances*" of the Data Transfer.[109] The DPC does not dispute its obligation to have regard to all the circumstances of the Data Transfers for the purpose of assessing any supplemental

[107] Response to the PDD, Part E, paragraph 3.9. See also Part E, paragraph 4.6(C).
[108] Response to the PDD, Part E, paragraph 3.11.
[109] Response to the PDD Part A, paragraph 2.4(A)(3) ; Part C, paragraphs 2.5, 3.13 ; Part E, paragraphs 3.1, 4.10(A), fn 162, 4.10(B). See also Part C, paragraph 2.3 ("*[t]he CJEU Judgment very clearly did not make any findings particular to FIL or the FIL Data Transfers*").

measures adopted. However, the first question—essential equivalence—requires an assessment of US law in circumstances in which the CJEU has already made binding conclusions on US law. It is simply not open to the DPC to ignore these conclusions.

7.134 In any event, the DPC does not accept Meta Ireland's assertions of a lack of completeness in the assessment undertaken by the DPC of the relevant circumstances.

7.135 In particular, for the purpose of the essential equivalence assessment, the DPC has identified and considered the critical circumstances relevant to this assessment:

(1) As set out above, the DPC has established that Meta Ireland's transfers at issue are to the US. This factor in turn compels the DPC to have regard to the findings on US laws and practices in the Judgment (as set out above);

(2) The DPC has identified that Meta Ireland is a company that is an electronic communications services provider, subject to Section 702 FISA and to the PRISM programme.

7.136 In its response, Meta Ireland has not disputed that the DPC is correct on both these matters and in fact has confirmed that it is subject to Section 702 FISA. Moreover, Meta Ireland has provided evidence to the DPC concerning the volumes of requests which it receives under Section 702 FISA over a three-year period and showing the number of requests and numbers of accounts affected by the requests.[110]

7.137 Consequently, the DPC is satisfied that, insofar as relates to the first part of the assessment—the essential equivalence analysis—it properly regards itself as bound by the findings in the Judgment. The DPC does not therefore regard it as necessary to engage in detail with the analysis set out in Annexure 2 to the Response to the PDD.

7.138 ***Sixth***, as regards Meta Ireland's argument that the DPC should undertake an up-to-date assessment of whether US law and practice is "*essentially equivalent*"[111], the DPC of course accepts that it must consider the impact of any developments in US law from the date of the Judgment. However, the DPC does not regard it as appropriate to undertake an entirely new assessment of all of the aspects of US law that were so comprehensively considered by the

[110] Response to the PDD, Part E, paragraph 3.11.
[111] See, e.g., Response to the PDD, Part A, paragraphs 2.4(A)(2), 2.4(C), 2.4(E); Part C, paragraph 3.5(2), 3.9; Part E, paragraphs 4.1, 4.3, 4.15, and 5.3.

CJEU in the Judgment. Indeed, it would be contrary to EU law for the DPC to disregard the findings of the CJEU on US law. For example, Meta Ireland makes the submission that:

> "*As explained in the EA, it is incorrect to conclude that no 'limitations on the power [Section 702 FISA] confers' exist. While such limitations were not discussed in the CJEU Judgment, the CJEU Judgment (an extract of which is quoted in the PDD) emphasises the need to examine both the 'law and practices in force in the third country'. When an up-to-date assessment is conducted on this basis, it is clear that Section 702 FISA does in fact provide for a number of limitations and safeguards (as explained in the EA).*"[112]

7.139 However, it is simply not open to the DPC to second-guess the findings of the CJEU on Section 702 FISA.

7.140 Thus, the DPC certainly agrees that it is appropriate to assess legal developments post-dating the Judgment to assess whether they affect any of the findings made by the CJEU in the Judgment. However, apart from such developments, the DPC regards itself as bound by the findings in the Judgment.

7.141 The DPC has had full regard to the specified, recent changes in US law outlined in Meta Ireland's Response to the PDD[113], to include the USG's White Paper, and in its Response to the RPDD. The DPC has also fully considered the submissions made by the US Government, both in respect of the PDD and the RPDD. However, I am satisfied that there is nothing in those materials that undermines the analysis in the Judgment of the deficiencies in protection for EU persons when data is transferred from Meta Ireland to Meta US.

7.142 ***Seventh***, Meta Ireland's ongoing reliance on the Ombudsperson seems misplaced.[114] Meta Ireland notes that Annex A to the Privacy Shield Decision extended access to the Privacy Shield Ombudsperson to EU data subjects whose data had been transferred pursuant to SCCs.

7.143 The DPC accepts that Meta Ireland has maintained its certification as part of the Privacy Shield programme, and that the protections afforded to Data Users by the Ombudsperson remain available, including the handling of complaints from Data Users in relation to transfers made pursuant to SCCs.

---

[112] Response to the PDD, Part E, paragraph 4.6(C).
[113] Response to the PDD, Part G, paragraph 2.1(B).
[114] Response to the PDD, Part E, paragraph 4.7, p 60.

7.144 However, as Meta Ireland itself concedes, the CJEU concluded that the Ombudsperson mechanism did not provide any cause of action before a body which offers persons whose personal data is transferred to the US guarantees essentially equivalent to those required by Article 47 of the Charter given that:

(1) The Ombudsperson reports directly to the Secretary of State;

(2) The Ombudsperson is appointed by the Secretary of State (an integral part of the US State Department);

(3) There is nothing to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees or that the Ombudsperson could adopt binding on intelligence services; and

(4) There is no mention of any legal safeguards that would accompany the political commitment on which data subjects could rely.[115]

7.145 Consequently, it appears to me that Meta Ireland's reliance on the Ombudsperson is misplaced and I do not accept Meta Ireland's submission that this is a "*further factor that must be taken into account as a safeguard in assessing the level of protection afforded to [Meta Ireland] Users in relation to the [Meta Ireland] Data Transfers*".[116] Even if I am wrong about this, it is clear that the Ombudsperson does not address the deficiencies in the remedies available in the US such as to achieve "*essential equivalence*" with the remedies made available under EU law.

7.146 ***Eighth***, the DPC also regards Meta Ireland's reliance on the EU-UK Adequacy Decision ("**UK Adequacy Decision**") as misplaced.[117]

7.147 The DPC is not required to conduct a thorough comparison of the EU Commission's adequacy findings on the specifics of the UK regime versus the US.

7.148 However, without prejudice to this, Meta Ireland's submissions suggesting that the UK Adequacy Decision demonstrates that bulk collection does not, in itself, undermine the essential equivalence of a regime fail to take account of the other elements relating to

[115] Judgment, paragraphs 195–197.
[116] Response to the PDD, Part E, paragraph 4.7.
[117] Response to the PDD, Part E, paragraph 4.20.

oversight and enforceable data subject rights and the role of the UK's Information Commissioner's Office contained in the UK Adequacy Decision.

Meta Ireland's Factors Assessment

7.149 I have had full regard to Meta Ireland's Factors Assessment, as requested by Meta Ireland[118]. I am satisfied (and I so find) that this assessment does not address the deficiencies identified above and by the CJEU in US law.

7.150 Meta Ireland emphasises that it is transparent regarding government requests for user data.[119] However, transparency about the fact that data rights are infringed does not actually remedy the relevant infringements.

7.151 Insofar as Meta Ireland contends that requests for Users' data by the USG in the national security context are limited and proportionate in practice,[120] these submissions seem to simply ignore the ruling of the CJEU. For example, it is difficult to reconcile Meta Ireland's "*relevant and documented practical experience*" that requests from USG agencies "*do not amount to anything that could be considered 'bulk surveillance' but, on the contrary, are limited in nature to what is necessary and proportionate*",[121] with the finding of the CJEU that Section 702 FISA "*does not indicate any limitation on the power it confers*" (paragraph 180).

7.152 It is also difficult to reconcile the statement of Meta Ireland that "*[a]ll requests are also subject to the terms of an independent court-approved certification with minimisation requirements and ongoing court supervision*"[122], with the finding of the CJEU that "*the FISC does not authorise individual surveillance measures; rather it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)*".

7.153 Similarly, it is difficult to reconcile Meta Ireland's contention that "*disclosures are limited to what is necessary and proportionate*"[123] with the finding of the CJEU that Section 702 FISA "*does not indicate any limitation on the power it confers*" (paragraph 180).

[118] Response to the PDD, Part E, paragraph 3.2.
[119] Response to the PDD, Part E, paragraphs 3.3—3.8.
[120] Response to the PDD, Part E, paragraphs 3.9—
[121] Response to the PDD, Part E, paragraph 3.9.
[122] Response to the PDD, Part E, paragraph 3.10.
[123] Response to the PDD, Part E, paragraph 3.13.

7.154 It is noted that Meta Ireland notes that "*[i]f the request is unlawful, overly broad, or legally deficient in any way, [Meta Ireland] will challenge or reject the request*".[124] However, the reality is that the CJEU has found that all requests are overly broad and legally deficient such that compliance with same will result in breach of EU law. Thus, Meta Ireland's statement that it "*reviews the legality of requests… and produces data only in response to valid legal process*" (paragraph 3.13) means that, by definition, it is responding to requests that are in breach of EU law.

Whether the SCCs can Remedy the Inadequate Protection Afforded by US Law

7.155 Given my conclusion on US law, I must therefore proceed to consider the second issue, and whether the SCCs can remedy the inadequacies in protection just identified.

7.156 As a preliminary point, I consider it appropriate to focus my analysis on the 2021 SCCs rather than the 2010 SCCs, given that, as at the date of this Decision, the 2010 SCC Decision stands repealed, and Meta Ireland and Meta US have entered into the 2021 DTPA, effective from 31 August 2021, a central purpose of which was (and is) to ground the Data Transfers on the 2021 SCC Decision and the 2021 SCCs. It is also of course the case that the 2021 SCC Decision was adopted (and the 2021 SCCs developed) specifically with a view to implementing the terms of the Judgment.

7.157 Having regard to the temporal scope of the Inquiry, however, I will first set out, briefly, my findings on the question as to whether the 2010 SCCs can remedy the inadequacies in protection just identified.

The 2010 SCCs

7.158 I am satisfied that the issue has already been determined by the CJEU in the Judgment. In that regard, a critical finding of the CJEU is found at paragraph 126 of the Judgment. While I have already set it out above, it is useful to repeat it here. It is as follows:

> "*… although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses,* ***there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the***

[124] Response to the PDD, Part E, paragraph 3.13.

effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates."[125]

7.159 The CJEU has clearly found that in circumstances in which the law of a third country allows its public authorities to interfere with the rights of the data subjects to which that data relates, SCCs will not suffice to guarantee the necessary protection of the data.

7.160 Given that the CJEU found that US law interferes with the rights of data subjects under Articles 7, 8 and 47 of the Charter (as already set out above), it necessarily follows that SCCs cannot compensate for the inadequacies in the level of protection afforded by US law.

7.161 Given the clear findings of the CJEU, it does not appear to me that it is necessary to analyse this issue further.

7.162 However, I add that even if the CJEU had not made the finding at paragraph 126 of the Judgment, it is obvious that the 2010 SCCs cannot address inadequacies of the protection afforded by US law.

7.163 The particular deficiencies in protection arising in the context of the US—identified above—relate to US authorities acting in the national security context. As the CJEU observed, "*it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract*".[126]

7.164 Given that the 2010 SCCs do not bind the US authorities, they will be incapable of regulating processing undertaken by US authorities or of giving rise to an effective remedy for any interference, actually addressing the injury suffered by the data subject.

7.165 Rather, in light of Clause 5 and the footnote thereto in the 2010 SCCs, it is clear that the mandatory requirements of US law go beyond what is necessary in a democratic society and that compliance with same must be treated as a breach of the 2010 SCCs (as held in the Judgment).[127]

[125] Emphasis added.
[126] Judgment, paragraph 125.
[127] Judgment, paragraph 141.

7.166 It is also important to consider Meta Ireland's submission that "*it cannot follow that **any** interference with the rights of data subjects necessarily renders SCCs insufficient as a safeguard*".[128] It is not necessary for me to comment on this submission, given that, for reasons already set out, it is clear that the CJEU was satisfied that the ***particular*** interference arising here was not capable of being remedied by the SCCs.

7.167 I also reject Meta Ireland's suggestion that the DPC's reasoning appears to disregard "*another clear finding in the CJEU Judgment that 'the mere fact that standard data protection clauses … do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of [the 2010 SCC Decision]'*".[129] The DPC's reasoning does not disregard this finding. However, to reiterate, the fact remains that, in the circumstances arising here, for reasons already outlined, SCCs cannot remedy the deficiencies in US law. The DPC also relies in this regard on the statement of the CJEU at paragraphs 126 and 135 of the Judgment, as already set out above.

7.168 Accordingly, I am satisfied–and I so find–that the 2010 SCCs cannot compensate for the inadequate level of protection provided by US law.

The 2021 SCCs

7.169 The substance of analysis set out above in relation to the 2010 SCCs applies equally to the 2021 SCCs. That is to say, the 2021 SCCs do not implement any new measure(s) directed to (or compensating for) the specific deficiencies in US law as identified by the CJEU in the Judgment. Whilst the arrangements they provide for are unquestionably more developed than the 2010 SCCs, such developments are, in large part, procedural in nature, to include, for example, the requirement at Clause 14 pursuant to which a written assessment must be prepared by the exporting and importing party directed to issues relating to local laws and practices affecting compliance with the Clauses, to include local laws and practices requiring the disclosure of data to public authorities or authorising access by such authorities.

7.170 It remains the case therefore that, in circumstances where the CJEU has found that US law interferes with the rights of data subjects under Articles 7, 8 and 47 of the Charter (as already set out above), the 2021 SCCs cannot compensate for the inadequacies in the level of protection afforded by US law.

---

[128] Response to the PDD, Part C, paragraph 3.10(A).
[129] Response to the PDD, Part C, paragraph 3.10(B).

7.171 Contrary to what has been contended for by Meta Ireland, provisions in the 2021 SCCs said to impose "*more onerous obligations on data importers and exporters, such as in respect of notification to data subjects and handling of legal requests*", whilst important in their own right, do not change this analysis, or the analysis undertaken by the CJEU in the Judgment.

7.172 In particular, nothing in the 2021 SCCs changes the fact that Meta Ireland and/or Meta US is an electronic communications service provider subject at a minimum to the obligations imposed under the FISA 702 PRISM programme.

7.173 It is my view, therefore, that Meta Ireland's reliance on the 2021 SCCs (which are not, of course, binding on the USG) does not (and cannot) compensate for the deficiencies in US law identified in the Judgment.

Summary

7.174 In short, the position is as follows:

(1) Under the Section 702 FISA's known "downstream" programme (PRISM), there could be non-court supervised access to a user's data without their knowing;

(2) Meta Ireland cannot stop this with SCCs, whether it has incorporated the 2010 SCCs or the 2021 SCCs in its DTPA; and,

(3) There is no remedy for an EU data subject who is not informed that they have been the subject of a FISA 702 search.

Whether there are Supplemental Measures that could Address the Inadequate Protection Provided by US Law

7.175 In the Judgment, the CJEU made clear that, where SCCs (in isolation) are unable to provide adequate protection to data subjects, controllers who are making transfers to a third country are required to implement supplementary measures to ensure the level of protection guaranteed by EU law.[130]

[130] Paragraphs 132 to 134.

7.176 As has already been discussed, the supplemental measures introduced must not merely "*mitigate"* the deficiencies in US law, as Meta Ireland contends,[131] but must ensure that data subjects receive essentially equivalent protection to EU law.

7.177 In its Response to the PDD, Meta Ireland summarises the supplemental measures it has put in place and which it submits, when taken with the protective measures implemented through the 2021 SCCs, provide appropriate safeguards to data subjects.[132] The supplemental measures are also referred to in the Transfer Impact Assessment Summary. However, as those measures are set out in most detail in the Record of Safeguards and Supplementary Measures (**"ROS"**), I will focus my analysis on this document.[133]

7.178 In the ROS, Meta Ireland breaks down the measures it has in place (to include measures supplemental to the 2021 SCCs) into three categories: organisational measures; technical measures; and legal measures. I will adopt the same structure when considering whether these measures, taken in conjunction with the 2021 DTPA, provide appropriate safeguards in the context of data transfers made to the United States.

Organisational measures

7.179 The ROS refers to a number of organisational measures implemented by Meta Ireland and Meta US. The first section of the ROS considers a range of policies and procedures implemented by those parties. These include a Disclosure Policy; a Disproportionate Requests Policy; a Notification Policy; a Data Access Policy; Law Enforcement Guidelines; Facebook Transparency Reports; Data Sharing Policies; and a People Security Policy.

7.180 The ROS also refers to a number of oversight measures Meta US has in place. Under these measures:

(1) Meta US is required to promptly notify Meta Ireland where it receives a legally binding request from a US public authority unless it is prohibited by law from doing so;

(2) Meta US submits detailed reports to Meta Ireland on disclosures made on foot of US legal requests;

[131] Response to the PDD, Part C, Paragraph 3.12.
[132] See in particular, Response to the PDD, Part E paragraphs 6.10 to 6.15.
[133] I have also considered the original Record of Safeguards document submitted by Meta Ireland.

(3) Meta US applies certain Quality Assurance arrangements to the body of work undertaken by its Law Enforcement Response Team;

(4) Meta US has implemented Operational Compliance policies.

7.181 The ROS also identifies the teams that Meta US has in place to evaluate and review government requests including its Law Enforcement Response Team, its Law Enforcement Outreach Team and its Quality Audit Team.

Technical measures

7.182 The ROS identifies a number of technical measures implemented by Meta US and Meta Ireland.

7.183 It first refers to the Comprehensive Information Security Program (**"CISP"**) that Meta US has in place. This Program is described as protecting *"the confidentiality, [i]ntegrity, and availability of data stored on [Meta US's] systems, platforms and products*."

7.184 The ROS also details how Meta US has implemented security measures in respect of external safeguards. In particular, it makes reference to measures implemented to ensure the confidentiality of data in transit:

> *"Facebook employs industry standard encryption algorithms and protocols to secure and maintain the confidentiality of User Data in transit. Employing industry standard encryption algorithms enables Facebook to secure User Data in transit from access by third parties, including even the most sophisticated government agencies. As data moves from user devices to Facebook's global network, Facebook employs industry standard encryption algorithms and protocols, such as Transport Layer Security ("TLS") and Advanced Encryption Standard ("AES"), to safeguard data as it traverses between Facebook's privately owned infrastructure and public networks."*

7.185 In addition, the ROS points to other technical measures that have been implemented, including shared infrastructure between Meta US and Meta Ireland, asset management controls, arrangements for the management of Facebook employee mobile devices, the implementation of encryption on Facebook laptops, the deployment of cryptographic protection of passwords and third party security policies.

7.186 The ROS also refers to a number of security measures Meta US has implemented for internal processing including: access controls and audit logs, logging and monitoring policies, secure disclosure practices, configuration management policies, change management policies, vulnerability management policies and white hat programs.

7.187 Other technical measures referenced in the ROS include risk assessments of the Law Enforcement Response Team's access tools, regular auditing of security measures, and identity verification for Law Enforcement Officials who make requests to Meta US to access personal data. Meta US is also said to have implemented security compliance and risk policies, information security policies and security incident response policies. The ROS notes that Meta US has a security team in place encompassing several hundred individuals.

Legal measures

7.188 The ROS lists a number of legal measures Meta Ireland and Meta US have implemented in respect of the Data Transfers.

7.189 In the first place, the ROS points to the contractual rights conferred on data subjects under the 2021 DTPA and the 2021 SCCs. The ROS states that these legal measures provide *"enforceable rights and remedies"* to data subjects in ensuring Meta Ireland and Meta US's compliance with the 2021 SCCs.

7.190 The ROS refers to a number of reactive legal measures which are in place. For example, Meta US challenges requests received for disclosure of personal data which Meta US believes to be unlawful. In addition, it seeks to challenge unduly broad requests which it believes are not necessary and proportionate in a democratic society. The ROS also state where Meta US is prohibited by the US Government from providing notice to data subjects prior to disclosing the data, Meta US will use its best efforts to obtain a waiver from such a prohibition.

7.191 The ROS refers to a number of *proactive* legal measures which are in place. One such measure listed is that Meta US engages in lobbying to change laws and advocates for its users' rights. The ROS also states that, since the Judgment, Meta US has provided additional transparency to its users in respect of government agency requests.

Assessment of the measures outlined in the ROS

Organisational measures

7.192 I am satisfied (and I so find) that the organisational measures identified in the ROS, read with the 2021 DTPA, do not compensate (nor could they) for the deficiencies in US law identified by the CJEU in the Judgment and as outlined above.

7.193 Although it is acknowledged that Meta US's Disclosure Policy, its Disproportionate Requests Policy and Law Enforcement Guidelines represent *bona fide* attempts to mitigate the deficiencies identified in US law, these measures are not such as would compensate for those deficiencies and so, whether viewed in isolation, or in tandem with the 2021 SCCs and the full suite of measures outlined in the ROS, they do not provide essentially equivalent protection to that available under EU law against USG access to users' personal data via Section 702 FISA DOWNSTREAM (PRISM) requests. Ultimately, if the US Government makes a request which falls within the scope of Section 702 FISA, Meta US is required to disclose its users' personal data.

Technical measures

7.194 The DPC has come to the same view in respect of the technical measures described in the ROS, i.e. whether viewed in isolation, or in tandem with the 2021 SCCs and the full suite of measures outlined in the ROS, they do not provide essentially equivalent protection to EU law against the wide discretion the US Government has to access Meta US users' personal data via Section 702 FISA DOWNSTREAM (PRISM) requests.

7.195 Although I have not come to a final view on this point (and do not consider it necessary to do so for the reasons outlined earlier in this Decision), I note that the encryption measures implemented in respect of data in transit *may* provide appropriate safeguards in the context of Section 702 FISA UPSTREAM or EO 12333. Importantly, however, Meta US and Meta Ireland have not demonstrated that they have implemented technical measures which will provide appropriate safeguards to data subjects from Section 702 FISA DOWNSTREAM (PRISM) requests for data which is in turn collected through compelled assistance. I am of the view that none of the technical measures listed in the ROS provide appropriate safeguards in respect of such requests.

Legal measures

7.196 I am likewise satisfied (and I so find) that the legal measures identified in the ROS (to include both its reactive and proactive measures) do not compensate for the deficiencies in US law in issue, whether viewed in isolation, or along with the other measures described in the ROS and/or in the 2021 SCCs.

7.197 Ultimately, the position remains that, if a valid request is made by the US Government which falls within the Section 702 FISA (PRISM) programme, Meta US is obliged to release or provide access to its users' personal data. Neither the 2021 DTPA nor the 2021 SCCs provide an effective remedy to affected users as required by Article 47 of the Charter.

EDPB Supplemental Measures Recommendations

7.198 The DPC has carefully considered Meta Ireland's criticisms of the "*EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" adopted on 18 June 2021 and published on 21 June 2021 ("the **EDPB Supplemental Measures Recommendations**").[134] However, these criticisms do not affect my analysis.

7.199 ***First***, the EDPB Supplemental Measures Recommendations do not exclude a so-called risk-based approach (this was deliberately inserted after point 3 of the Executive Summary).

7.200 ***Second***, however, the pertinent point is that Meta Ireland is not in a position to demonstrate that, notwithstanding the deficiencies in US law referenced in this Decision, in fact, no interference with EU rights occurs. Such interference does occur, and Meta Ireland does not have a remedy for it. In that regard, the risk-based approach called out by Meta Ireland as being identified in the GDPR can have no application where the essence of one or more of the Charter-based rights engaged is not respected.

7.201 ***Third***, Meta Ireland criticises the EDPB Essential Guarantees Recommendations on the basis that they do not mention the "*margin of appreciation*" under the ECHR.[135] However, as has already been addressed above, the relevant analysis must be conducted by reference to EU law and the Charter, not by reference to the ECHR. Moreover, the "*margin of appreciation*" has no equivalent in EU law and is not relevant for present purposes. Furthermore, the

[134] Response to the PDD, Part C, paragraph 7, p 78.
[135] Response to the PDD, Part E, paragraph 4.11(A).

position under EU law on bulk interception regimes is clear and has already been considered above. Given that the relevant benchmark is EU law, rather than ECtHR law, Meta Ireland's observation that the EDPB Essential Guarantees Recommendations pre-dated the Grand Chamber's decisions in *Big Brother Watch* and *Centrum för Rättvisa* are also not persuasive.[136]

Summary

7.202 In summary, therefore, I am satisfied (and I so find) that:

(1) US law does not provide a level of protection that is essentially equivalent to that provided by EU law;

(2) Neither the 2010 SCCs nor the 2021 SCCs can compensate for the inadequate protection provided by US law; and

(3) Meta Ireland does not have in place any supplemental measures which would compensate for the inadequate protection provided by US law.

7.203 Accordingly, in making the Data Transfers, I find that, subject to the analysis contained at Section 8 below, Meta Ireland is infringing Article 46(1) GDPR.

8. DEROGATIONS

8.1 The provisions of Article 49 GDPR are set out in detail in Part 5 of this Decision. Accordingly, I will not repeat them here.

8.2 I have carefully considered the submissions made by Meta Ireland in relation to its intended reliance on the derogations under Article 49 GDPR.[137]

8.3 I note that Meta Ireland has made detailed submissions in relation to its intended reliance on the 'contractual necessity' derogation under Article 49(1)(b) GDPR. I understand Meta Ireland to say that, if this legal basis for transfers was rejected, it would seek to rely on the public interest derogation under Article 49(1)(d) GDPR or, in the alternative, certain other of the derogations under Article 49 GDPR, or it would seek to procure the consent of Meta Ireland

[136] Response to the PDD, Part E, paragraph 4.12.
[137] Response to the PDD, Part F pages 87 – 103.; Meta Ireland's Reply to Schrems' Submissions, Part D; Response to the RPDD, Part C pages 23 – 39.

users in the EU/EEA to the transfer of their personal data to the United States under and by reference to the consent derogation at Article 49(1)(a) GDPR.

8.4 In its Response to the RPDD,[138] Meta Ireland submits that the approach to Article 49 GDPR in the RPDD is "*manifestly incorrect*" and "*wrong as a matter of law*".[139] I do not accept that characterisation, which is premised on a number of fundamental misunderstandings by Meta Ireland. I have nevertheless, for completeness, addressed Meta Ireland's intended reliance on Articles 49(1)(b), 49(1)(d) and 49(1)(a) GDPR separately below.

8.5 For the avoidance of doubt, I accept that, in the absence of an adequacy decision pursuant to Article 45(3) GDPR, or of appropriate safeguards pursuant to Article 46 GDPR, the derogations provided for under Article 49 GDPR may be relied on to make transfers to third countries which do not satisfy the "*essential equivalence*" standard. Meta Ireland's characterisation of Chapter 8 of the RPDD to the contrary is incorrect.

8.6 However, for the reasons that follow, I am satisfied that Meta Ireland cannot rely on the derogations under sub-paragraphs (b), (d) or (a) of Article 49 GDPR, or any derogation under Article 49 GDPR, to justify the scale of data transfers it is currently making from the EU to the US.

Interpretation and Application of Article 49 GDPR

8.7 Prior to addressing the derogations under Article 49 GDPR that Meta Ireland places reliance on, it is useful to outline the basis on which I am required to interpret and apply those derogations, in particular in light of Article 52(1) of the Charter.

Obligation to interpret and apply EU law measures in accordance with the Charter

8.8 I note that secondary EU law must be interpreted in conformity with primary law as a whole, including the Charter.[140] Where the wording of secondary EU law is open to more than one interpretation, preference should be given to the interpretation that renders the provision consistent with the Charter.[141]

[138] Response to the RPDD, 29 April 2022, Part C
[139] Response to the RPDD, Part C, Paragraph 1.2
[140] Article 6(1) TEU provides that the Charter shall have the same legal value as the Treaties.
[141] See, e.g., C-77/17, C-391/16, C-78/17 M and Others, paragraph 77 and the cases cited; Case C-817/19 Human Rights League v Council of Ministers, paragraph 86 and the cases cited.

8.9 Further, Article 51(1) of the Charter requires Member States to respect the fundamental rights enshrined in the Charter when implementing EU law. The CJEU has confirmed that Member States, and in particular Courts, must not rely on an interpretation of secondary EU law that would be in conflict with the fundamental rights protected by the Charter when implementing EU law.[142] I am satisfied that this requirement applies equally to the DPC.

8.10 I am therefore required to interpret and apply EU law – including the derogations under Article 49 GDPR – in accordance with the fundamental rights enshrined in the Charter, and in particular in light of Article 52(1) of the Charter.

Restrictive interpretation of derogations

8.11 It is well established that, in light of the foregoing, derogations from fundamental rights must be strictly construed.

8.12 ***First***, the CJEU has confirmed that the protection of fundamental rights guaranteed under the Charter requires that derogations from and limitations on those rights must apply only in so far as is strictly necessary, and must be narrowly construed.[143]

8.13 ***Second***, and relatedly, it is well established that derogations cannot be interpreted so as to allow the exception provided by the derogation to replace the rule established by the EU measure; it is necessary that *"the exception remain an exception."*[144]

8.14 In that respect, where a provision: "*provides for an exception to the general rule [it must] be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle … to become the rule, if [the rule] is not to be rendered largely meaningless*."[145]

8.15 ***Third***, the CJEU has confirmed that while derogations may be,

> " … *formulated in terms which are* ***sufficiently open to be able to adapt to different scenarios*** *and keep pace with changing circumstances … the Court may, where appropriate, specify, by means of interpretation,* ***the actual scope of the limitation*** *in*

[142] See e.g., C-133/19 and C-136/19 B.M.M v Etat belge, paragraph 33 and the cases cited; C-411/10 and C-493/10 N.S. v Secretary of State for the Home Department, paragraph 77 and the cases cited.
[143] See, e.g., C-212/13 Ryneš, paragraphs 28 – 29 and the cases cited.
[144] C-623/17 Privacy International, paragraph 69 and the cases cited.
[145] C-149/20 Dwyer v Commission for An Garda Síochána, paragraph 40 and the cases cited.

the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, ***as interpreted in view of the fundamental rights guaranteed by the Charter.***"[146]

8.16 I am required to interpret and apply the derogations under Article 49 GDPR in accordance with those principles.

Article 52(1) of the Charter and the 'essence' of the right

8.17 In addition, I must interpret and apply Article 49 GDPR in accordance with Article 52(1) of the Charter. Any derogation from a right guaranteed by the Charter, whether that derogation is set out in an EU measure or otherwise, must comply with Article 52(1) of the Charter, which provides:

> "*1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*."

8.18 Article 52(1) of the Charter therefore identifies three cumulative requirements with which any limitation on or derogation from a Charter right must comply. Derogations are permissible only where they: "*first, are 'provided for by law', secondly, respect the 'essence' of that freedom* ***and****, thirdly, respect the principle of proportionality*."[147]

8.19 A derogation that does not respect the "*essence*" of a fundamental right must therefore be considered invalid, without it being necessary to examine the third condition in Article 52(1) of the Charter, relating to compliance with the principle of proportionality.

8.20 Advocate General Saugmandscaard Øe expressed that principle as follows:

> "*98. It should be recalled that the condition, set out in Article 52(1) of the Charter, that any limitation on the exercise of the rights and freedoms recognised by that instrument must 'respect the essence of those rights and freedoms' means that,* ***where a measure undermines that 'essence', it cannot be justified****. That measure*

[146] Case C-817/19 Ligue des droits humains, paragraph 114 and the cases cited.
[147] Opinion of Advocate General Saugmandscaard Øe in Case C-401/19 Republic of Poland v European Parliament, delivered on 15 July 2021

is then deemed to be contrary to the Charter and, in the case of an act of the European Union, it must be annulled or declared invalid ***without it being necessary to examine the condition relating to compliance with the principle of proportionality****.*

99. Indeed, the EU legislature may limit the exercise of certain fundamental rights in the common interest in order to protect other rights and interests. It may do so, in particular, in order to protect another fundamental right. In that context, it has a certain margin of discretion to weigh up and strike a 'fair balance' between the various rights and interests involved. Nevertheless, there is an absolute limit to that margin of discretion. ***The 'essence' of a fundamental right is an 'untouchable core' which must remain free from any interference****. Accordingly, no objective, however legitimate it may be, justifies certain – exceptionally serious – interferences with fundamental rights. In other words, the end does not justify all means*."[148]

8.21 That principle was recently reiterated by Advocate General Giovanni Pitruzzella, as follows:

"91. It is apparent, in particular, from the judgment of 6 October 2015, Schrems, that the failure by a Union act to respect the essence of a fundamental right ***automatically*** *entails its nullity or invalidity, without there being any need to balance the interests at stake. The Court thus recognises that every fundamental right has a "hard core", ensuring that everyone can have a sphere of freedom which is protected from any interference by the public authorities and which cannot be restricted, except by challenging the principles of democracy, the rule of law and respect for human dignity which underlie the protection of fundamental rights.* ***Furthermore, it is apparent both from the wording of Article 52(1) of the Charter and from the case-law of the Court, in particular the Schrems I judgment, that the assessment of whether there has been an interference with the essence of the fundamental right at issue must be made prior to and independently of***

[148] Opinion of Advocate General Saugmandscaard Øe in Case C-401/19 Republic of Poland v European Parliament, delivered on 15 July 2021, paragraphs 98-99. The CJEU applied that principle, proceeding to determine the proportionality of the EU measure at issue only after determining that the EU measure respected the 'essence' of the right to freedom of expression and information guaranteed in Article 11 of the Charter (paragraphs 76-81). See also Opinion of Advocate General Saugmandscaard Øe in Case C-311/18 Schrems II, paragraph 272.

the assessment of the proportionality of the measure in question. *In other words, it constitutes a test having its own autonomous status."*[149]

8.22 I am therefore required to interpret and apply Article 49 GDPR as precluding derogations that do not comply with the *"essence*" of a fundamental right. It is only where a derogation from a fundamental right respects the "*essence*" of that right that it is necessary to proceed to a balancing test.

Transfers to the US and interference with the 'essence' of Charter rights

8.23 In the Judgment, the CJEU determined that identified laws that permit data surveillance in the United States do not respect the "*essence*" of the right to an effective judicial remedy under Article 47 of the Charter.

8.24 In its Response to the RPDD, Meta Ireland submits that the Judgment makes no finding that there has been an interference with the "*essence*" of any fundamental right.[150] For the reasons outlined below I do not agree.

8.25 The Response to the RPDD also suggests that I reached the conclusion that there was an interference with the "*essence*" of the right to an effective judicial remedy, based only on the CJEU's conclusion there was a lack of "*essential equivalence*" in the United States, conflating those concepts.[151]

8.26 For the avoidance of doubt, I did not in the RPDD, and do not now, conflate a lack of "*essential equivalence*", with an interference with the "*essence*" of a fundamental right. In that regard, it is acknowledged that a finding to the effect that the law of a third country does not ensure a level of protection that is "*essentially equivalent*" to that guaranteed by EU law does not mean, without more, that an interference with the *"essence"* of a fundamental right has been established.

8.27 My conclusion that identified laws that permit data surveillance in the United States do not respect the "*essence*" of the right to an effective judicial remedy under Article 47 of the Charter

[149] Opinion of Advocate General Guivanni Pitruzzella in Case C-817/19 Human Rights League v Council of Ministers delivered on 27 January 2022 (translated from the French version of that Opinion, where an English version is unavailable). Again, the CJEU applied that principle in its decision, proceeding to determine the proportionality of the EU measure at issue only after determining that the EU measure respected the 'essence' of the right at issue.
[150] Response to the RPDD, Part D, paragraph 3.2
[151] Response to the RPDD, Part C, paragraph 3.5

is not therefore based on or inferred from the Court's finding of a lack of "*essential equivalence*". Rather, it is based on the CJEU's finding in the Judgment that there is an interference with the essence of that right.

8.28 In light of those submissions by Meta Ireland, I will outline in more detail the basis for that conclusion. In that respect, the treatment of this issue in the judgment in Case C-362/14, and the preliminary questions referred to the CJEU and at issue in the Judgment, lend useful context.

The judgment in Case C-362/14: The Safe Harbour Decision

8.29 In its judgment in Case C-362/14, the CJEU noted with respect to Article 47 of the Charter, when striking down the European Commission's Safe Harbour Decision, that:

> *" … legislation* ***not providing for any possibility for an individual to pursue legal remedies*** *in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data,* ***does not respect the essence of the fundamental right to effective judicial protection****, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law."*[152]

8.30 The CJEU also indicated (referencing paragraph 39 of its earlier decision in Digital Rights Ireland) that where a surveillance programme permits or facilitates access on a generalised basis to the content of electronic communications, such programme will be regarded as compromising the "*essence*" of an individual's fundamental right to privacy under Article 7 of the Charter.[153]

8.31 On that basis the CJEU held that the Safe Harbour decision was invalid, without engaging in a proportionality analysis under the second sentence of Article 52(1) of the Charter.

[152] C-362/14 Schrems, paragraph 95.
[153] C-362/14 Schrems, paragraph 92.

The Questions Referred

8.32 Following the judgment in Case C-362/14, the Commissioner undertook a merits-based assessment of the Complaint and, following delivery of the Prior Draft Decision, issued proceedings in the High Court in which the court was invited to make a reference to the CJEU for a preliminary ruling *"on the validity of [the 2010 SCC Decision and related implementing decisions of the European Commission] insofar as they apply to data transfers from the European Economic Area to the United States, having regard to the Charter, and in particular, to Article 7 and/or Article 8 and/or Article 47 thereof."*

8.33 With respect to Article 47 of the Charter, the High Court reached a conclusion expressed in the following terms:

> "*To my mind the arguments of the DPC that the laws - and indeed the practices - of the United States* ***do not respect the essence of the right to an effective remedy*** *before an independent tribunal as guaranteed by Article 47 of the Charter, which applies to the data of all EU data subjects transferred to the United States, are well founded. Furthermore, even if the essence of that right is respected, there are, for the reasons advanced by the DPC, well founded concerns that the limitations on the exercise of that right faced by EU data subjects in the United States* ***are not proportionate*** *and are not strictly necessary within the meaning of Article 52 (1) of the Charter*."[154]

8.34 By order of 4 May 2018, the High Court made a reference for a preliminary ruling to the CJEU. I note that Question 4 and Question 5 as referred to the CJEU were as follows:

> *"4. Given the facts found by the High Court in relation to US law, if personal data is transferred from the EU to the US under the SCC Decision does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?*
>
> *5. Given the facts found by the High Court in relation to US law, if personal data is transferred from the EU to the US under the SCC Decision:*

[154] The High Court Judgment, paragraph 298.

(a) ***Does the level of protection afforded by the US respect the essence of an individual's right to a judicial remedy*** *for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?*

If the answer to (a) is yes,

(b) ***Are the limitations imposed by US law on an individual's right to a judicial remedy*** *in the context of US national security* ***proportionate within the meaning of Article 52 of the Charter*** *and do not exceed what is necessary in a democratic society for national security purposes?"*

8.35 I note in particular, with respect to the questions referred, that the CJEU was asked expressly to determine: (i) whether the "*essence"* of Article 47 of the Charter was respected, and (ii) if the "*essence*" of Article 47of the Charter *was* respected, whether any limitations on Article 47 were proportionate within the meaning of Article 52 of the Charter.

<u>The Judgment</u>

8.36 It is acknowledged that the Judgment did not hold that the "*essence*" of Article 7 or Article 8 Charter rights were interfered with by limitations on the protection of personal data arising from the domestic law of the United States. Rather, the CJEU held that those limitations failed to meet the proportionality requirement under the second sentence of Article 52(1) of the Charter.[155]

8.37 In contrast, however, when the Judgment is read as a whole, it is clear that the CJEU did determine that identified laws that permit data surveillance in the United States do not respect the "*essence*" of the right to an effective judicial remedy under Article 47 of the Charter.

8.38 ***<u>First</u>***, in paragraph 187 of the Judgment, the CJEU referenced its findings in its judgment in C-362/14, with respect to when the "*essence"* of the right to an effective judicial remedy under Article 47 of the Charter will be interfered with:

[155] With respect to Article 7 and 8 rights, the CJEU confirmed that it was not ascertaining whether limitations on the protection of personal data arising from the domestic law of the United States complied with the first sentence of Article 52(1) (i.e. the "rule of law" and "essence" requirements), where the conclusion of the Commission in that respect was called into question on the basis of the second sentence of Article 52(2) (i.e. the proportionality requirement).

"*187. According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus,* ***legislation not providing for any possibility for an individual to pursue legal remedies*** *in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data,* ***does not respect the essence of the fundamental right*** *to effective judicial protection, as enshrined in Article 47 of the Charter (judgment of 6 October 2015,* ***Schrems, C-362/14****, EU:C:2015:650, paragraph 95 and the case-law cited)*."

8.39 ***Second***, the CJEU held that the lack of *any* redress mechanism as regards, in particular, E.O. 12333, made it ***impossible*** having regard to the case-law set out in paragraph 187 – i.e. the finding in its judgment in C-362/14 that legislation "*not providing for any possibility for an individual to pursue legal remedies*" does not respect the "*essence*" of the right to effective judicial protection – to make a finding of essential equivalence:

"191. … Thus, as regards E.O. 12333, the Commission emphasised, in recital 115, ***the lack of any redress mechanism. In accordance with the case-law set out in paragraph 187 above****, the existence of such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that presidential decree makes it* ***impossible*** *to conclude, as the Commission did in the Privacy Shield Decision, that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter."*

8.40 ***Third***, the CJEU continued, in paragraph 192:

"*192. Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that* ***data subjects have no right to an effective remedy***."

8.41 I am satisfied, in particular having regard to the express reliance by the CJEU on the principle identified in the CJEU's judgment in C-362/14, as set out in paragraph 187 of the Judgment – that legislation not providing for any possibility for an individual to pursue legal remedies does not respect the "*essence*" of the right to effective judicial protection – when concluding that a finding of effective equivalence was *impossible*, that these paragraphs represent a clear finding

by the CJEU that, in the context of EU-US data transfers, identified legislation in the United States does not respect the "*essence*" of the fundamental right to effective judicial protection.

8.42 My conclusion in that respect is reinforced by the fact that the CJEU did not (in contrast to its treatment of Articles 7 and 8 of the Charter) proceed to engage in any proportionality exercise with respect to Article 47 of the Charter. This is despite the question referred to the CJEU expressly *requesting* a finding on proportionality, if the CJEU were satisfied that the "*essence*" of the right to effective judicial protection under Article 47 of the Charter was respected by the United States domestic measures.

8.43 I have carefully considered Meta Ireland's argument that the CJEU did not in fact identify a breach of the essence of any Charter right.[156] Having regard to the foregoing, I do not accept that argument. I am satisfied that when the Judgment is read as a whole, that finding is clear.

8.44 I am also satisfied that nothing turns on the fact that the Court's analysis was undertaken by reference to the Privacy Shield Decision, rather than the SCCs. Ultimately, it is clear that the Court was satisfied, for the reasons set out in the Judgment, that in the context of transfers to the United States, identified laws applicable in that jurisdiction operate in such a manner as to interfere with the essence of EU citizens' fundamental right to an effective remedy under Article 47 of the Charter.

8.45 In the circumstances, I am satisfied, bearing in mind the following matters, that when considering whether the derogations set out at Article 49(1) GDPR are available to (and can be relied on by) Meta Ireland in respect of the systematic, bulk, repetitive and ongoing transfers comprised within the Data Transfers, I must have regard to the following:

a. For the reasons noted in the Judgment, identified laws of the United States interfere with the essence of EU citizens' fundamental right to an effective remedy under Article 47 of the Charter.

b. Any measure that interferes with the essence of a fundamental right, cannot be justified (and is not subject to any proportionality balancing exercise).

[156] Response to the RPDD, Part C, paragraph 3.3 et seq; Part D, paragraph 3.2

c. Meta Ireland's Response to the PDD acknowledges that it has received (and continues to receive) requests from the US Government, with which it is bound to comply (and does in fact comply), to disclose the content of data subjects' communications.[157]

d. Reliance by Meta Ireland on the derogations at Article 49 GDPR (which, as a matter of principle, must apply only insofar as is strictly necessary, and cannot be applied so as to permit the exception to become the rule) falls to be considered in the same way as reliance on any measure that would interfere with the essence of a fundamental right.

8.46 I will now address the three sub-paragraphs of Article 49 GDPR on which Meta Ireland seeks to rely.

Article 49(1)(b) GDPR: 'Contractual Necessity'

8.47 I am satisfied that the contractual necessity derogation cannot be relied on to justify the systematic, bulk, repetitive and ongoing transfers to the US comprised within the Data Transfers, for the following reasons.

8.48 ***First***, the CJEU has held that the legal regime in the US governing redress where individuals, including EU data subjects, have been the subject of unlawful surveillance for national security purposes under certain legislation fails to respect the "*essence"* of the right to effective judicial protection.

8.49 Meta Ireland proposes to rely on this derogation to continue the systematic, bulk, repetitive and ongoing transfers to the United States comprised within the Data Transfers. This will result in the personal data of EU data subjects being transferred to the United States and subjected to a legal regime that does not respect the "*essence"* of the rights guaranteed by Article 47 of the Charter, without the consent of those data subjects to that interference with their Article 47 Charter rights.

8.50 It follows that the contractual necessity derogation cannot be interpreted and/or applied to permit the systematic, bulk, repetitive and ongoing transfers comprised within the Data Transfers, where the transfers thereby effected would give rise to a breach of the *essence* of a fundamental right of EU/EEA users. No proportionality balancing exercise arises in that respect.

[157] Response to the PDD, Part E, paragraph 3.11.

8.51 Meta Ireland submits that this reasoning is fundamentally flawed, as it amounts to an argument that Article 49 GDPR cannot be relied on for transfer to a country that lacks an *"essentially equivalent"* level of protection.

8.52 However, this is to misunderstand the position.

8.53 I accept that data can be transferred under the contractual necessity derogation to a third country that does not ensure a level of protection that is "*essentially equivalent*" to that guaranteed by the EU, but that nevertheless respects the *"essence"* of the fundamental rights arising, provided that transfer meets the requirements of Article 49(1)(b) GDPR and subject to the proportionality test in the second line of Article 52(1) of the Charter.

8.54 However, that is not the situation that arises here.

8.55 As I have observed, a finding by the CJEU that there has been an interference with the *"essence"* of a fundamental right is comparatively rare; it is the exception, not the rule. However, where such a finding is made by the CJEU – as it has been with respect to identified laws in the United States – I am required, in accordance with Article 52(1) of the Charter, to interpret and apply the Article 49 GDPR derogations, including the Article 49(1)(b) GDPR derogation, accordingly.

8.56 In those circumstances, I find that the contractual necessity derogation cannot be relied on to justify the Data Transfers.

8.57 ***Second***, even if the proposed reliance on the contractual necessity derogation did not give rise to a breach of the essence of Article 47 of the Charter, I am satisfied that systematic, bulk, repetitive and ongoing transfers are not in any event permitted under Article 49(1)(b) GDPR.

8.58 In this regard, it is of note that Recital 111 of the GDPR describes transfers made in the context of the "*contractual necessity*" and "*legal claims*" derogations[158] as being "occasional". The EDPB Guidelines state – and I agree – that, in light of Recital 111, Articles 49(1)(b), (c) and (e) GDPR can be relied on to justify "*occasional*" transfers only.

[158] Sub-paragraphs (b), (c) and (e) of Article 49(1).

8.59 Such an approach is unsurprising in circumstances where, as a general point of EU law, it is well-established that derogations are to be interpreted narrowly[159], and any restrictions or derogations from the rights guaranteed in Articles 7 and 8 of the Charter will be permissible only insofar as *"strictly necessary".*[160] As the EDPB has correctly observed, and as held by the CJEU on many occasions[161], such a position is necessary to avoid a situation in which the exception may become the rule.[162]

8.60 Meta Ireland submits that the EDPB Guidelines are incorrect in that respect, and that this interpretation is incompatible with the terms of Article 49 GDPR. In making that submission, they rely, *inter alia*, on the following:

a. The non-binding nature of the preamble to EU measures;

b. The legislative history of Article 49 GDPR, and

c. Changes made to the EDPB Supplemental Measures Recommendations.

8.61 I have considered each of those arguments carefully. However, for the reasons set out below, I remain of the view that the EDPB guidelines are correct and that Article 49(1)(b) GDPR can justify "*occasional*" transfers only.

The non-binding nature of preambles

8.62 Meta Ireland argues that where the limitation on derogations under Article 49(1)(b) GDPR to "*occasional*" transfers is stated in Recital 111 of the GDPR only, and is not repeated in Article 49 GDPR, it has no effect.

8.63 It is acknowledged that the preamble to an EU law measure does not have the same status as an operative provision. Meta Ireland is correct that the preamble of an EU Act has no binding

[159] See, for example, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, at paragraph 52 and Case C-362/14 *(Schrems)* at paragraph 92.
[160] Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd ECLI:EU:C:2020:559 paragraph 176; Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications ECLI:EU:C:2014:238 paragraph 52; Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB ECLI:EU:C:2016:970; Case-362/14 paragraph 96; Schrems v Data Protection Commissioner ECLI:EU:C:2015:650; Case C-623/17 Privacy International ECLI:EU:C:2020:790 paragraph 81; Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net ECLI:EU:C:2020:791 paragraph 130.
[161] C-149/20 Dwyer v Commission for An Garda Síochána, paragraph 40 and the cases cited. Case C-817/19 Ligue des droits humains, paragraph 114 and the cases cited.
[162] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (Adopted on 25 May 2018) page 4.

legal force and cannot be relied on as a ground for either derogating from the actual provisions of the act, or for interpreting those provisions in a matter that is clearly contrary to their wording. This is well established in the CJEU jurisprudence, including in the cases cited by Meta Ireland.

8.64 However, it is also well established that the recitals of an EU act: "*may explain the content of the provisions of that act*", and that recitals "*constitute important elements for the purposes of interpretation, which may clarify the intentions of the author of that act*."[163]

8.65 In that respect, I note that in Case C-528/16 *Confédération paysanne and Others EU:C:2018:583,* the CJEU relied on Recital 17 of the GMO Release Directive[164] to inform the limitations of a derogation under that Directive. Article 3(1) of the GMO Release Directive provides that the Directive shall not apply to organisms obtained through the techniques of genetic modification listed in Annex 1 B. One of the techniques listed in Annex 1 B is "*mutagenesis*".

8.66 No limitation on the type of mutagenesis excluded from the scope of the Directive is contained in Article 3 or Annex 1 B. The CJEU nevertheless interpreted the limitations on the scope of that derogation in light of Recital 17, which provides:

> "*This Directive should not apply to organisms obtained through certain techniques of genetic modification* ***which have conventionally been used in a number of applications and have a long safety record****."*

8.67 In light of that Recital the CJEU held:

> *"Article 3(1) of Directive 2001/18, read in conjunction with point 1 of Annex I B to that directive and in the light of recital 17 thereof, must be interpreted as meaning that only organisms obtained by means of techniques/methods of mutagenesis* ***which have conventionally been used in a number of applications and have a long safety record*** *are excluded from the scope of that directive."*

8.68 In reaching that conclusion the CJEU relied on, *inter alia,* the following:

---

[163] Case C-418/18 *P Puppinck and others v Commission of the European Communities,* paragraph 75

[164] Directive 2001/18/EC of the European Parliament and of the Council of 12 March 2001 on the deliberate release into the environment of genetically modified organisms and repealing Council Directive 90/220/EEC

a. That as "*a provision derogating from the requirement to subject GMOs to the obligation laid down in the Directive*", Article 3(1), read in conjunction with Annex 1 B, "*must be interpreted strictly*";[165]

b. That for the purpose of interpreting a provision of EU law, it is necessary to consider not only its wording but also "*the context in which it occurs and the objectives pursued by the rules of which it is part*";[166]

c. That by *"referring generally to mutagenesis",* that provision does not, on its own, *"provide any conclusive guidance as to the types of techniques/methods that the EU legislature intended specifically to exclude from the scope of the directive"*;[167]

d. That the EU legislature set out in recital 17 "*the conditions under which certain GMOs should be excluded from the scope of the Directive*" and that, "*accordingly, the scope of the derogation … **must be determined in the light of the clarifications thus given by the EU legislature***";[168] and

e. That an interpretation of the derogation that did not exclude techniques that had not conventionally been used in a number of applications and have a long safety record would fail to have regard to the intention of the EU legislature, reflected in recital 17, and would compromise the objective of the Directive.[169]

8.69 I have also considered the authorities relied on by Meta Ireland. I accept that those authorities establish that a recital cannot be relied on to derogate from the actual provisions of the act in question, or to interpret those provisions in a manner that it clearly contrary to their wording. However, I do not accept that Recital 111 of the GDPR either derogates from Article 49(1)(b) GDPR or results in an interpretation of Article 49(1)(b) GDPR that is clearly contrary to its wording. Rather, recital 111 of the GDPR serves to clarify the scope of the derogation permitted under Article 49(1)(b) GDPR.

[165] Paragraph 41
[166] Paragraph 42
[167] Paragraph 43
[168] Paragraphs 44-46
[169] Paragraphs 51-53

8.70 Further, I do not accept that the authorities cited by Meta Ireland require – or could justify – an interpretation of Article 49(1)(b) GDPR that ignores the clear legislative intent demonstrated in Recital 111 of the GDPR. The EU legislature set out in Recital 111 of the GDPR the conditions under which certain transfers should be excluded from the requirements in GDPR Chapter IV and *"accordingly, the scope of the derogation … must be determined in the light of the clarifications thus given by the EU legislature*." I am satisfied that interpreting the limitations of the scope of Article 49(1)(b) GDPR in light of Recital 111 of the GDPR is entirely consistent with the approach taken by the CJEU in *Confédération paysanne.*[170]

The legislative history

8.71 Meta Ireland also rely on the legislative history of the GDPR, in particular with respect to the insertion – or failure to insert – a limitation based on frequency or volume of transfers in Article 49 GDPR, other than with respect to the "*legitimate interest*" derogation.

8.72 I do not accept that this means that Article 49 GDPR should not be interpreted in light of Recital 111 of the GDPR. Regard must also be had to the legislative history of Recital 111 itself. I note, in that respect, that the requirement that transfers under the "*contractual necessity*" derogation be "*occasional*" was not included in the preamble to the Directive. Nor was included in the first proposal with respect to the GDPR. It was introduced during the GDPR legislative process and, in that respect, cannot be considered to be unintentional or inadvertent.[171] On the contrary, it must be considered to represent the legislative intent with respect to the limitations of the scope of the derogation under Article 49(1)(b), (c) and (e) GDPR. I do not accept Meta Ireland's submission that it should simply be disregarded.

Amendments to the EDPB Supplemental Measures Recommendations

8.73 Finally, I do not find Meta Ireland's reliance[172] on the amendments between the initial draft of the EDPB Supplemental Measures Recommendations and the final draft to be convincing. The text in the original draft reads:

[170] See also, e.g., C-424/10 and C-425/10 Ziolkowski v Land Berlin, paragraphs 42 and 43
[171] See, by analogy, C-424/10 and C-425/10 Ziolkowski v Land Berlin, paragraph 43
[172] Response to the RPDD, §6.19(B), Draft EDPB Supplemental Measures Recommendations, Executive Summary on page 2 and paragraph 25 on page 11. EDPB Supplemental Measures Recommendations, Executive Summary on page 3 and paragraph 25 on page 13

"*Only in some cases of **occasional and non-repetitive transfers** you may be able to rely on one of the derogations provided for in Article 49 GDPR, if you meet the conditions*."[173]

8.74 The text in the amended draft reads:

*"Only in some cases you may be able to rely on one of the derogations provided for in Article 49 GDPR if you meet the conditions. **Derogations cannot become "the rule" in practice, but need to be restricted to specific situations**."*[174]

8.75 A similar change was made later in the document.

8.76 It is uncontroversial – and has at all times been reflected in the EDPB Guidelines – that the reference to "*occasional*" in Recital 111 of the GDPR applies to sub-paragraphs (b), (c) and (e) of Article 49(1) GDPR only, and that the reference to "*non-repetitive*" applies to the "*legitimate interest*" derogation only. However, the well-established principle that a derogation cannot become "*the rule*" in practice, reflected in the final draft of the EDPB Regulations, applies to all Article 49 derogations. In those circumstances, I do not accept that the change in language can reasonably be interpreted as indicating that the EDPB has altered its clear and unequivocal position that the contractual necessity derogation under Article 49(1)(b) GDPR applies only with respect to "*occasional*" transfers. I am reinforced in that conclusion by the fact that the final EDPB Supplemental Measures Recommendations, which provide only a short reference to the Article 49 GDPR derogations, expressly refer the reader to the EDPB Guidelines for more detailed guidance on those derogations.[175] That is not, in my view, consistent with Meta Ireland's submission that the EDPB has changed its position on the relevance of Recital 111 of the GDPR.

8.77 I therefore do not accept Meta Ireland's submission that the EDPB Guidelines misinterpret the scope of the derogation under Article 49(1)(b) GDPR. I am satisfied that Article 49(1)(b) GDPR can relied on to justify "*occasional*" transfers only.

8.78 ***Third***, I note Meta Ireland's emphasis on paragraph 202 of the Judgment, where the Court stated that the consequence of invalidating the Privacy Shield Decision *"is not liable to create such a legal vacuum"* on account of the derogations in Article 49 GDPR. I understand Meta

[173] Draft EDPB Supplemental Measures Recommendations, Executive Summary on page 2
[174] Draft EDPB Supplemental Measures Recommendations, Executive Summary on page 2
[175] EDPB Supplemental Measures Recommendations, paragraph 25 on page 13

Ireland to say that this observation is to be taken to mean that the Court considered that some or all of the derogations would be available to Meta Ireland.

8.79 In my view, that contention is not well-founded, either with respect to Article 49(1)(b) GDPR or otherwise, particularly in light of a number of other statements of principle contained elsewhere in the Judgment. In that regard, I consider that it is important to have regard to the Judgment in determining whether or not the derogations provided for at Article 49(1) GDPR – including the derogation at Article 49(1)(b) GDPR – are available to Meta Ireland for, or in connection with, the Data Transfers.

8.80 In particular, and whilst acknowledging that the point was made in the context of the Court's analysis of Article 46 GDPR, it is nonetheless of significance that, at paragraph 92 of the Judgment, the CJEU observed that the baseline level of protection contemplated by Article 44 GDPR must be guaranteed irrespective of the particular transfer mechanism relied on to make a given transfer or set of transfers. The Court expressed this point in the following terms:

> *"Although Article 46 of the GDPR does not specify the nature of the requirements which flow from that reference to 'appropriate safeguards', 'enforceable rights' and 'effective legal remedies', it should be noted that that article appears in Chapter V of that regulation and, accordingly, must be read in the light of Article 44 of that regulation, entitled 'General principle for transfers', which lays down that 'all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined'. That level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out."*

8.81 If the derogations at Article 49(1) GDPR – including Article 49(1)(b) GDPR – could properly be relied on by Meta Ireland as providing a lawful basis for the systematic, bulk, repetitive and ongoing transfer of users' data from the EU to the US, such an outcome would not simply be in tension with the Court's findings in the Judgment as they relate to US law (and, in particular, its finding to the effect that the Data Transfers give rise to a breach of the essence of the rights conferred on Meta Ireland's users by Article 47 of the Charter), but would set those findings at nought.

8.82 Having regard to the Court's statements in relation to the baseline level of protection applicable, uniformly, across all transfer methods provided for in Chapter V, and noting the

Court's statements (elsewhere in the Judgment) presaging the mandatory suspension or prohibition of transfers, to include, for example, that set out at paragraph 146 of the Judgment[176], I am satisfied that the Court did not have it in mind that one or more of the derogations might conceivably be used, in effect, to side-step its core findings in relation to US law and, further, that, in the light of the Judgment, and having regard to all of the circumstances of the Data Transfers, any contention to the effect that one or more of the derogations – including Article 49(1)(b) GDPR – might be relied on to justify systematic, bulk, repetitive and ongoing transfer of users' data from the EU to the US, is not sustainable.

8.83 Having regard to the foregoing, it is my conclusion (and I so find) that Meta Ireland cannot rely on the "*contractual necessity"* derogation under Article 49(1)(b) GDPR to justify the systematic, bulk, repetitive and ongoing transfers comprised within the Data Transfers.

Article 49(1)(d) – the public interest derogation

8.84 Meta Ireland submits that, in the event that its position regarding reliance on Article 49(1)(b) GDPR is not accepted, it will rely on the public interest derogation under Article 49(1)(d) GDPR. It is my conclusion (and I so find) is that Meta Ireland cannot rely on Article 49(1)(d) GDPR to justify the Data Transfers, for broadly the same reasons it cannot rely on Article 49(1)(b) GDPR.

8.85 ***First,*** for the reasons set out above, with respect to Meta Ireland's proposed reliance on Article 49(1)(b) GDPR, I do not accept that Article 49(1)(d) GDPR can be interpreted or applied so as to permit the systematic, bulk, repetitive and ongoing transfers comprised within the Data Transfers, where the transfers thereby effected would give rise to a breach of the *essence* of the fundamental rights of EU/EEA users. No balancing exercise arises in that respect.

8.86 For the avoidance of doubt, I again clarify that the reason no balancing exercise arises is because permitting Meta Ireland to rely on the derogation under Article 49(1)(d) GDPR to justify the Data Transfers would not respect the "*essence*" of the rights guaranteed by Article 47 of the Charter. Were reliance to be placed on Article 49(1)(d) GDPR to make transfers to a third country that does not satisfy the "*essential equivalence*" standard, but that nevertheless

[176] The statement to which reference is made is as follows: *"…unless there is a valid Commission adequacy decision, the competent supervisory authority is* ***required****, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer, if, in its view and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer."* As will be apparent, in describing the competent supervisory authority's obligations in this context, the Court did not use discretionary language.

respects the "*essence"* of the rights guaranteed by the Charter, I accept it would be necessary to engage in a balancing exercise under the second sentence of Article 52(1) of the Charter, having regard in particular to the public interests relied on. However, that is not the situation here.

8.87 ***Second,*** I am in any event satisfied that Article 49(1)(d) GDPR cannot be relied upon to justify the systematic, bulk, repetitive and ongoing transfers comprised within the Data Transfers. Whilst it is acknowledged that Recital 111 of the GDPR does not explicitly state that the derogation at Article 49(1)(d) GDPR[177] is to apply solely to "*occasional*" and/or "*non-repetitive*" transfers, I note and agree with the following observations made by the EDPB:

> *"Nonetheless, it has to be highlighted that even those derogations which are not expressly limited to "occasional" or "not repetitive" transfers have to be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place."*[178]

8.88 Again, that conclusion is supported by the well-established principle that derogations must be interpreted strictly, and cannot be interpreted so as to allow the exception provided by the derogation to replace the rule established by the EU measure. The case for a narrow interpretation of the derogations in Article 49(1) GDPR is reinforced by the wording of the title to Article 49 GDPR itself, which indicates that the derogations are to be used for ***"specific situations"***.[179]

8.89 ***Third,*** I again note that if the derogations at Article 49(1) GDPR – including the derogation at Article 49(1)(d) GDPR – could properly be relied on by Meta Ireland as providing a lawful basis for the systematic, bulk, repetitive and ongoing transfer of users' data from the EU to the US, such an outcome would not simply be in tension with the Court's findings in the Judgment as they relate to US law, but would set those findings at nought. Again, I am of the view that this

[177] Or the "explicit consent derogation" at Article 49(1)(a), the "vital interests derogation" at Article 49(1)(f) or the "register" derogation at Article 49(1)(g).
[178] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (Adopted on 25 May 2018) page 5.
[179] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (Adopted on 25 May 2018) page 4. Emphasis added.

supports an interpretation of Article 49(1)(d) GDPR that does not permit the systematic, bulk, repetitive and ongoing transfer of users' data from the EU to the US.

8.90 Accordingly, I am satisfied that it is not open to Meta Ireland to rely on the derogation at Article 49(1)(d) GDPR in the context (or for the purpose of) systematic, bulk, repetitive and ongoing transfers of its users' data from the EU to the US.

Article 49(1)(a) – Explicit consent

8.91 Finally, Meta Ireland indicates that, to the extent that its reliance on Article 49(1)(b) and (d) GDPR is not accepted, "it would likely seek to obtain and rely upon the explicit consent" of EU/EEA users to the Data Transfers.

8.92 As will be apparent, Meta Ireland has not in fact obtained the explicit consent of EU/EEA users to any of the Data Transfers at this point. It follows, therefore, (and I so find), that Meta Ireland cannot rely on the derogation under Article 49(1)(a) GDPR to justify the Data Transfers.

8.93 Whether Meta Ireland could rely on Article 49(1)(a) GDPR to justify *any* of the Data Transfers in the future, if it were to obtain the explicit consent of EU/EEA users, cannot be determined in the abstract.

8.94 I have, nonetheless, carefully considered Meta Ireland's submissions on this issue and, in so doing, I have identified a number of points of principle on which I believe I can and, indeed, should, set out my views at this point.[180]

8.95 In that regard, I acknowledge that Article 8 of the Charter recognises the importance of consent, with respect to the processing of data. I further recognise that Recital 7 of the GDPR states that "Natural persons should have control of their own personal data".

8.96 I also accept, as a matter of principle, and having regard to the foregoing, that it may be possible for reliance to be placed on Article 49(1)(a) GDPR to justify a transfer or set of transfers to the US, where all of the requirements of that sub-article are complied with.

[180] For the avoidance of doubt, these views are necessarily preliminary in nature and do not form part of the operative parts of my decision. Moreover, they are not intended (and should not be considered to reach) any conclusion on the matters at hand, reflecting the fact that there is no scheme before me under which Meta Ireland contends that it collects the explicit consent of EU/EEA Users sufficient to justify any proposed transfer of Users' personal data to the United States. In the event that, at some future date, Meta Ireland adopts such a scheme, the DPC would consider the lawfulness of same on its merits and afford Meta Ireland a reasonable opportunity to address (amongst other things) the statements of position set out – on a preliminary basis - herein.

8.97 Although identified legislation in the United States does not respect the "essence" of Article 47 Charter rights, I accept that that does not necessarily or automatically mean that a derogation that permits a specific transfer of data to the United States, subject to explicit and fully informed consent in accordance with Article 49(1)(a) GDPR, will interfere with the "*essence*" of that fundamental right.

8.98 This is because, in order to obtain explicit consent under Article 49(1)(a) GDPR to "*the proposed transfer"*, it is necessary that the data subject is "*informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards".*

8.99 In the context of transfers to the United States, this would require that the data subject be informed, in addition to the information that would be provided for 'normal' consent, *inter alia*: (i) that the data will not be subject to equivalent protection to that afforded by Article 7 and Article 8 of the Charter, (ii) that identified laws in the United States interfere with the essence of Article 47 Charter rights with respect to that data, and (iii) of the possible risks of the proposed transfer to the data subject.[181] If explicit and fully informed consent in accordance with Article 49(1)(a) GDPR is obtained from the data subject to "*the proposed transfer",* and therefore to that interference with his or her Article 47 Charter rights, I accept in principle that such a transfer cannot be said to interfere with the *"essence"* of that data subject's right under Article 47 of the Charter.

8.100 However, I note that it is unclear how, on a practical level, Meta Ireland could justify *all* of the Data Transfers based on Article 49(1)(a) GDPR in the event that it sought to put in place a scheme by which the explicit consent of EU/EEA Users to any proposed transfer of their personal data to the United States was obtained, sufficient to meet the requirements laid down in Article 49(1)(a) GDPR and elsewhere in the GDPR. In particular, it is my preliminary view that a single consent by an EU/EEA data subject could not be sufficient to justify any and all future transfers of that user's personal data to the US.

[181] This, in addition to the requirement for explicit consent with respect to the proposed transfer, is in my view the key distinction with respect to the contractual necessity derogation. Although in the context of the contractual necessity derogation, the data subject must be informed pursuant to Article 13(1)(f) and (14)(1)(f) that the controller intends to transfer personal data to the third country and of the absence of an adequacy decision, there is no requirement to obtain consent in that respect – still less explicit consent – nor is the data subject informed of the risks arising as a result of that transfer.

8.101 In that regard, there is a high threshold for obtaining any consent under the GDPR.[182] The threshold for obtaining consent under Article 49(1)(a) GDPR is even higher. In particular:

a. The data subject must have "*explicitly consented*" to "*the proposed transfer*", and

b. The data subject must have been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

8.102 The requirement that consent be "*explicit"* for the "*contractual necessity*" derogation is newly introduced in the GDPR, and raises the threshold with respect to the quality of consent as compared to the equivalent derogation in the Directive, which required only that the consent be "*unambiguous"*.

8.103 My preliminary view is that the requirement that consent be "*explicit"* and that it relate to "*the proposed transfer"* precludes a single consent being obtained for ongoing data transfers and/or different sets of transfers. I am also of the view that seeking a single consent for ongoing data transfers and/or different sets of transfers is not compatible with the obligation to inform the data subject of the possible risks of the transfers being made. Further, interpreting Article 49(1)(a) GDPR to allow such an approach would be inconsistent with the well-established principle that derogations must be interpreted narrowly, and the exception must not be permitted to become the rule, and would again be to set the decision of the CJEU in the Judgment at naught.

8.104 Finally, and for completeness, I also note in this regard – and agree with – the statement in the EDPB Guidelines that:

> "*2.1.2 Consent must be specific for the particular data transfer/set of transfers*
>
> *One of the requirements of valid consent is that it must be specific. In order to constitute a valid ground for a data transfer pursuant to Article 49(1)(a), hence, consent needs to be specifically given for the particular data transfer or set of transfers.*
>
> *…*
>
> *Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer at the time of the collection of the data, e.g. if the*

[182] See, e.g., Recitals 32, 42, 43, Article 4(11), Article 7

occurrence and specific circumstances of a transfer are not known at the time consent is requested, the impact on the data subject cannot be assessed."

The Balance of the Derogations

8.105 Meta Ireland has not sought to rely on the balance of the derogations at Article 49 GDPR. It follows, therefore, that no issue arises for determination in relation thereto. For completeness, however, I would observe that it would not appear to be open to Meta Ireland to rely on those other derogations, when it is not clear how they could be engaged in connection with the Data Transfers in the first place, and where, in any event, broadly the same reasons as those set out above in connection with the derogations at Article 49(1)(b) and (d) GDPR would also appear to apply the remaining derogations cited within that Article.

Conclusion and Finding

8.106 In light of the foregoing, I find that it is not open to Meta Ireland to rely on the derogations at Article 49(1) GDPR (or any of them) to justify the systematic, bulk, repetitive and ongoing transfer of users' data from the EU to the US.

9. CORRECTIVE MEASURES

9.1 It is my view that, for the reasons outlined below, it is necessary to exercise corrective powers in order to address the infringement identified above and that, in all the circumstances, it is appropriate, necessary and proportionate to order the suspension of the Data Transfers pursuant to Article 58(2)(j) GDPR.

Obligation of an EU controller or processor to suspend EU/US data transfers

9.2 The responsibility to ensure that data transfers are only made in circumstances in which a level of protection is ensured that is essentially equivalent to that provided by the GDPR, read in light of the Charter, falls in the first instance on the EU controller or processor.

9.3 In particular, the CJEU held in the Judgment that, where a controller or a processor established in the EU is not able to take adequate additional measures to guarantee the required

protection, the controller or processor "*or, **failing that**, the competent supervisory authority*" are required to suspend or end the transfer of personal data to the third country concerned.[183]

9.4 Significantly, the CJEU added that:

> "*[t]his is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union **obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access** by the public authorities of that third country to that data*".[184]

9.5 The CJEU also observed that:

> *"[i]n the light of the requirements of Article 46(1) and (2)(c) of the GDPR, read in the light of Articles 7 and 8 of the Charter, **the controller is bound to suspend the transfer of data** and/or to terminate the contract where the recipient is not, or is no longer, able to comply with the standard data protection clauses. Unless the controller does so, it will be in breach of its obligations under Clause 4(a) in the annex to the SCC Decision as interpreted in the light of the GDPR and of the Charter."*[185]

9.6 The Advocate General also referred to the obligation on the controller to suspend the proposed transfer.[186]

9.7 The EDPB Supplemental Measures Recommendations likewise identify the obligation to suspend or end the transfer of personal data in such circumstances.[187]

9.8 Thus, it is only where the EU controller fails to guarantee the required protection, that the supervisory authority is required to take action. Furthermore, the corrective measure chosen by the DPC must be viewed in light of Meta Ireland's obligations in this regard.

[183] Judgment, paragraph 135. Emphasis added.
[184] Judgment, paragraph 135. Emphasis added.
[185] Judgment, paragraph 140. Emphasis added.
[186] Opinion, EU:C:2019:1145, paragraph 144.
[187] EDPB Supplemental Measures Recommendations, e.g., paragraph 57.

Corrective Measure

9.9 For the reasons set out above, and having considered the relevant circumstances of the Data Transfers, to include, *inter alia*, the "factors" assessment and Record of Safeguards contained in the TIA, I am satisfied that:

(1) US law does not provide a level of protection that is essentially equivalent to that provided by EU law;

(2) Neither the 2010 SCCs nor the 2021 SCCs can compensate for the inadequate protection provided by US law;

(3) Those of the measures set out in the Record of Safeguards that forms part of the TIA that are presented or characterised as supplemental to the measures for which provision is made in the 2010 SCCs and/or 2021 SCCs, do not compensate for the inadequate protection provided by US law; and

(4) It is not open to Meta Ireland to rely on the derogations provided for at Article 49(1) GDPR (or any of them) when making the Data Transfers.

9.10 Accordingly, I have found that, in making the Data Transfers, Meta Ireland is infringing Article 46(1) GDPR.

9.11 I also note Meta Ireland's reference to the EDPB statement that supervisory authorities are:

> "*required to assess individual cases, either ex officio or following a complaint, and to either refer the case to a national Court if they suspect that the transfer does not comply with Article 45 where there is an adequacy decision,* ***or to suspend or prohibit the transfer if they find Article 46 GDPR cannot be complied with and the protection of the data transferred required by EU law cannot be ensured by other means***".[188]

9.12 I agree with this statement.

9.13 I also note that Meta Ireland appears to suggest that suspension of data transfers is not required in all cases where there is non-compliance with Article 46 GDPR. As a general point,

[188] Response to the PDD, Part E, paragraph 4.10(B).

I agree with this, but only where protection can be "*ensured by other means*". I am not satisfied that such "*other means*" have been demonstrated by Meta Ireland.

9.14 Given that the Data Transfers have not been suspended or ended by Meta Ireland, the DPC has available to it a range of corrective powers under Article 58(2) GDPR.

9.15 I accept Meta Ireland's submission that the DPC is required to exercise any corrective power in a manner that is "*appropriate, necessary and proportionate*"[189], taking into account the circumstances of the individual case.

9.16 However, I do not accept Meta Ireland's submission regarding the nature of the proportionality assessment required in the context of exercising a corrective power. Meta Ireland correctly notes that the need to balance the right to the protection of personal data against other fundamental rights is expressly recognised in Recital 4 GDPR. However, Meta Ireland submits that a further such balancing of rights is required by Recital 129 GDPR, after an infringement of the GDPR has already been established and corrective measures are being considered. Meta Ireland therefore submits that the DPC must conduct the balancing exercise both when interpreting the provisions of the GDPR (e.g., Article 49 GDPR) and when considering the use of corrective powers.[190] Meta Ireland submits that it cannot be said that the GDPR itself incorporates the relevant balancing exercise, even if Meta Ireland acknowledges that Recital 4 GDPR supports such an interpretation.[191] I do not accept Meta Ireland's submissions in this regard.

9.17 Recital 4 GDPR provides that the right to the protection of personal data must be "*balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.*"

[189] Response to the PDD, Part G, paragraph 2.4, citing GDPR Recital 129.
[190] Response to RPDD dated 29 April 2022, Part D, paragraph 3.2.
[191] Response to RPDD dated 29 April 2022, Part G, paragraph 3.1.

9.18 The analysis of whether Article 46 GDPR has been breached is conducted within the framework of the GDPR and as such, insofar as appropriate, relevant fundamental rights are balanced accordingly.[192] I have determined that Article 46 GDPR has been (and is being) breached. That determination is the product of, *inter alia*, a proportionality-based assessment embedded in the legislative scheme.

9.19 Meta Ireland submits that, notwithstanding this determination, a further balancing of rights must take place before a corrective measure is adopted. In particular, Meta Ireland submits that a suspension order would be wholly disproportionate to furthering the aim of protecting users against any "*practical risk of undue interference*" with their data protection rights.[193] This submission overlooks the fact that the relevant balancing exercise has (insofar as required) taken place and it effectively seeks to avoid the consequences of the determination that Article 46 GDPR has been breached.

9.20 In support of this submission, Meta Ireland refers also to the requirement to reconcile the right to the protection of personal data with the right to freedom of expression and information. However, this requirement is embedded into the scheme of the GDPR, rather than required as part of an assessment for the purposes of Article 58(2) GDPR. Section 43 of the 2018 Act, which gives effect to this requirement, provides for an exemption from compliance with a broad range of provisions of the GDPR where compliance would be incompatible with the said rights.

9.21 Instead, what is required when considering the adoption of corrective measures under Article 58(2) GDPR is an assessment of what is "*appropriate, necessary and proportionate in view of ensuring compliance with*" the GDPR.[194] To conduct a further balancing of rights as suggested by Meta Ireland would not be appropriate at this stage as it carries with it the possibility that an infringement of the GDPR would be permitted to continue. The assessment of whether there has been a breach of the GDPR will have already taken place prior to consideration of the appropriate corrective measure. Under the proper legislative scheme, once the breach has been established, it is for the supervisory authority to adopt those corrective measures (if any) which are appropriate and necessary to ensure compliance with the GDPR, but which are also proportionate to the relevant infringement.

---

[192] It is noted that, in the circumstances of this case, as discussed above in section 8, the essence of the right in question has been breached and, accordingly, there is no need to carry out a balancing exercise between other interests that may be engaged.
[193] Response to RPDD dated 29 April 2022, Part G, paragraph 1.2.
[194] Recital 129 GDPR.

9.22 If the imposition of a corrective measure required to ensure compliance with the GDPR were subject to the kind of proportionality assessment put forward by Meta Ireland – and thereby potentially allowed the breach to continue – the general legislative scheme and policy would be significantly undermined. Meta Ireland submits that an appropriate and proportionate corrective measure in the circumstances is something less than suspension of the Data Transfers, but that cannot be so if it permits the ongoing infringement of the GDPR.

9.23 It is my view that the corrective measure I have determined to apply – suspension of the Data Transfers – is necessary but no more than necessary in order to ensure compliance with the GDPR. As stated in the Judgment, if "*a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy.*"[195]

9.24 In such circumstances, although it is for the DPC to "*determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its* ***responsibility for ensuring that the GDPR is fully enforced with all due diligence****.*"[196] The DPC is therefore required to take appropriate action in order to remedy the identified (and ongoing) breach of Article 46 GDPR.

9.25 In all the circumstances, I am satisfied that it is appropriate, necessary and proportionate to invoke the power under Article 58(2)(j) GDPR to order the suspension of the Data Transfers. It also clearly emerges from the Judgment that, in circumstances such as these, it is appropriate for a supervisory authority such as the DPC to suspend or end invalid data transfers.

9.26 In that regard, the CJEU endorsed the observation of the Advocate General in his Opinion[197] that the supervisory authority is required, under Article 58(2)(f) and (j) GDPR, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the 2010 SCCs are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be

[195] Judgment, paragraph 111.
[196] Judgment, paragraph 112. Emphasis added.
[197] Opinion, EU:C:2019:1145, paragraph 146.

ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.[198]

9.27 I accept Meta Ireland's submission that the CJEU stated in the Judgment (at paragraph 113) that supervisory authorities should suspend any data transfer if "*in light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means*". I have considered all of the relevant circumstances of the Data Transfers above, in Section 6, and have reached my view on the appropriate corrective measure accordingly.

9.28 Insofar as I am required to exercise any corrective power in a manner that is "*appropriate, necessary and proportionate*", taking into account the circumstances of the individual case, I consider that the following points arise in the particular circumstances of the present case:

(1) In the Judgment, the CJEU has made findings to the effect that certain of the infringements it identified (most notably those relating to the absence of any effective remedy[199]), give rise to a breach of the essence of a fundamental right, namely, the fundamental right to effective judicial protection, as protected by Article 47 of the Charter.

(2) Where a measure compromises the essence of a fundamental right, it is *per se* incompatible with the Charter, without there being a need to carry out a balancing exercise between such competing interests (if any) as may also be engaged.

(3) In the circumstances, and noting Meta Ireland's position that, if it cannot make the Data Transfers, it would not be in a position to maintain the provision of its services in the EU/EEA, the exercise of any corrective power other than one directing the temporary or permanent cessation of the offending transfers would result in a situation where the essence of a fundamental right of Users would be compromised on an ongoing and indefinite basis. On no view could such an outcome, the upshot of which would be to set Users' rights under Article 47 of the Charter at nought, be considered acceptable, much less permissible under law.

[198] Judgment, paragraph 113; see also paragraph 146.
[199] See, for example, paragraphs 181, 187 and 192 of the Judgment.

(4) That view is not undermined by any of the factors identified at Part G, paragraph 2.20 of the Response to the PDD, or any of the impacts identified at paragraphs 3.4 through 3.11 thereof.

(5) As I have noted above, the Court has made clear in its Judgment[200] that, if, in a case where a transfer of personal data to a third country is not subject to an adequacy decision, a competent supervisory authority comes to the view that, in the light of all the circumstances of the transfer in question, the SCCs are not or cannot be complied with in that third country, and where (as here) the protection of the data transfers that is required by EU law cannot be ensured by other means, the competent supervisory authority is required, under Article 58(2)(f) and (j) GDPR, to suspend or prohibit such transfer.

9.29 It is accepted that, consistent with the requirement that any corrective measure be appropriate, necessary and proportionate, where "*there is a choice between several appropriate measures recourse must be had to the least onerous*".[201] It is important to note that the appropriateness of the relevant measures is determined by reference to the objective to be achieved. In this instance, the objective is to ensure compliance with the GDPR in circumstances where, in making the Data Transfers, Meta Ireland has (from the date of delivery of the Judgment on 16 July 2020), infringed, and is presently infringing, Article 46 GDPR.

9.30 I expressed the view, in the Draft Decision, that it was clear (and the relevant principles also emerge clearly from the Judgment) that the only corrective measures that are adequate to achieve the said objective are the banning or suspension of the Data Transfers. Accordingly, I noted my view, in the Draft Decision, that the DPC had a choice between two appropriate measures, and the DPC chose, in the Draft Decision, to order the suspension of the Data Transfers because that is the least onerous measure that ensures compliance with the GDPR. Such other measures as suggested by Meta Ireland do not ensure compliance with the GDPR.

9.31 It is submitted by Meta Ireland that the suspension order is disproportionate in circumstances where the DPC ought first to engage with Meta Ireland and explore what steps and actions might be adopted in order to make the Data Transfers compliant with Chapter V GDPR.[202] It is

[200] Judgment, paragraph 146 (inter alia)
[201] Case C-311/18 *Fedesa*, paragraph 13.
[202] Response to RPDD, Part G, paragraphs 2.21 and 2.22.

respectfully observed that an appropriate level of engagement has already taken place and Meta Ireland has had sufficient opportunity to satisfy the DPC regarding compliance.

9.32 Meta Ireland also relies on the observation of the DPC that a suspension order is more appropriate than a ban because, if measures become available to make the Data Transfers compliant, then the suspension could be re-considered. Meta Ireland submits that if such measures are capable of addressing the deficiencies, it must be afforded the opportunity to implement them prior to finalising any decision to suspend the Data Transfers.[203] However, it must be observed that Meta Ireland has not made any such proposals in the course of the Inquiry and that one of the purposes of the suspension order is to keep that opportunity open. In the circumstances, I neither agree nor accept that I am obliged, in effect, to stay the making of a decision to afford Meta Ireland a further opportunity to make fresh proposals in terms of achieving compliance with the requirements of the GDPR as they apply to the Data Transfers.

9.33 I also note the submission by Meta Ireland that to proceed with the suspension order at a point in time when an agreement in principle is said to have been reached between the European Commission and the USG regarding a new framework for transatlantic data flows would be inappropriate, unnecessary and disproportionate.[204] However, I do not accept that submission in circumstances where the DPC is under an obligation to give effect to the law as it currently stands[205].

9.34 Part D of the Response to the PDD sets out in detail Meta Ireland's views on the many rights that are engaged and, in Meta Ireland's view, promoted by the Data Transfers.

9.35 The DPC accepts that Users can avail themselves of the Facebook Service to engage in:

(1) Freedom of expression;

[203] Response to RPDD, Part G, paragraphs 4.2 and 4.3.
[204] Response to RPDD, p.8, paragraph 12; Part D, paragraph 1.5.
[205] For the avoidance of doubt, I am aware (and have considered) whether EO 14086 (and associated Regulations made by the US Department of Justice which, amongst other things, establish a Data Protection Review Court), bear on the matters addressed (and determined) in this Decision. For the reasons outlined at paragraphs 2.56 to 2.65, above, I am satisfied that, as matters stand, the answer to that question is no; the DPC is under an obligation to give effect to the law as it *currently* stands. As noted above, I am also aware that the European Commission published a draft implementing decision on 13 December 2022 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. Again, as matters stand, that decision has not yet been adopted and, accordingly, it does not bear on the issues addressed in this Decision.

(2) The right to respect for private and family life;

(3) The freedom to conduct a business;

(4) Freedom of thought, conscience and religion; and

(5) Freedom of the arts and sciences.[206]

9.36 It is also accepted that Meta Ireland enjoys freedom conduct a business and to "*peaceful enjoyment of [its] possessions*".[207]

9.37 I do not accept, however, that the other rights to which reference is made above would be "*severely adversely impacted*" if the Data Transfers were suspended such that, on the basis of a proportionality-balancing exercise, it necessarily follows that a suspension of the Data Transfers would be disproportionate.[208] In answer to criticisms levelled in Meta Ireland's Response to the RPDD (at Part D, Section 4), I would note that such an analysis assumes, not just that a proportionality-balancing exercise is required (it is not) but also that the suspension of the Data Transfers can properly be identified (and has been established as) the proximate cause of any such adverse impact (it has not).

9.38 I also note the reference of the CJEU in *Privacy International* (at paragraph 72) to the fact that:

> " … *the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter. Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistle-blowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ 2019 L 305, p. 17). Moreover, that deterrent effect is all the more serious given the quantity and breadth of the data retained (see, to that effect, judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 28; of 21 December 2016, Tele2, C-203/15 and C-698/15,*

[206] Response to the PDD, Part D, paragraph 1.4.
[207] Response to the PDD, Part D, paragraph 1.5.
[208] Response to the PDD, Part D, paragraph 3.4; see also paragraphs 1.3, 1.4, 1.9.

EU:C:2016:970, paragraph 101; and of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, paragraph 118)."

9.39 It is of note that, in the present case, the deficiencies in US law themselves have an impact in undermining the protection afforded to the other fundamental rights to which Meta Ireland refers.

9.40 Additionally, it is of note, not just that an order directing the suspension of the Data Transfers would not be targeted at the suite of "other" rights identified by Meta Ireland in its Response to the PDD, but that, on Meta Ireland's own case, any compromising of those other rights would arise as a result of the architecture of the systems developed and deployed by Meta Ireland in the delivery of its services. In that regard, it is noted that Meta Ireland makes the point that, at least in their current configuration, its systems do not and/or cannot make provision for the delivery of its services in the EU/EEA without the Data Transfers.

9.41 In any event, the critical issues here are that the deficiencies in US law identified by the CJEU have not been addressed by the SCCs or supplemental measures, that a derogation under Article 49(1) GDPR is not available to Meta Ireland, and that the Data Transfers have been found to give rise to a breach of the essence of one or more fundamental rights.

9.42 Given the circumstances of the Data Transfers and all of the other factors outlined above, and having considered the provisions of Article 83(2) GDPR, I am satisfied, and I so find that a suspension of data transfers is appropriate and proportionate.

9.43 In this respect, I regard as relevant:

(1) The importance of the rights at issue, namely Articles 7, 8 and 47 of the Charter;

(2) The very clear inadequacies in US law identified by the CJEU;

(3) The fact that neither the 2010 SCCs nor the 2021 SCCs can compensate for those inadequacies;

(4) Those of the measures set out in the Record of Safeguards that forms part of the TIA that are presented or characterised as supplemental to the measures for which provision is made in the 2010 SCCs and/or 2021 SCCs, do not compensate for the inadequate protection provided by US law;

(5) The fact that it is not open to Meta Ireland to rely on the derogations provided for at Article 49(1) GDPR (or any of them) when making the Data Transfers;

(6) The clear emphasis in the Judgment on suspension and banning of data transfers in circumstances such as those arising here; and

(7) The fact that suspension is necessary to ensure that the ongoing interferences with the rights of data subjects (to include a breach of the essence of certain of those rights) are brought to an end as soon as possible.

9.44 I note that Meta Ireland criticises the DPC for relying "*almost exclusively on statements in the CJEU Judgment*" in adopting a preliminary view in the PDD that suspension would be appropriate.[209] This is not accepted.

9.45 I therefore find that it is appropriate that the Data Transfers be suspended pursuant to my powers under Article 58(2)(j) GDPR.

9.46 For completeness, I clarified, in the Draft Decision, that I did not propose to impose a permanent ban on the Data Transfers, recognising that new measures, not currently in operation, may yet be capable of being developed and implemented by Meta Ireland and/or Meta US to compensate for the deficiencies identified herein. I noted, in the Draft Decision, that if that situation were to arise, I would then be in a position to reconsider the suspension. I concluded, in the Draft Decision, that suspension therefore appeared to me to be a proportionate response in all the circumstances, and one that was more appropriate than (for example) an order directing Meta Ireland to bring its processing operations as they relate to the Data Transfers into compliance with the requirements set out in Chapter V of the GDPR, read in the light of the Charter. In that regard, I noted again, in the Draft Decision, Meta Ireland's stated position that, if it cannot make the Data Transfers, it would not be in a position to provide its services in the EU/EEA.

9.47 I also had regard, in the Draft Decision, to the DPC's power to impose an administrative fine, whether in addition to, or instead of, any of the other measures set out in Article 58(2) GDPR. In that regard, I carefully considered the criteria set out in Article 83(2)(a)–(k) GDPR.

9.48 I expressed the view, in the Draft Decision, that the imposition of an administrative fine in addition to an order directing the suspension of the Data Transfers would not be "*effective,*

[209] Response to the PDD, Part G, paragraph 2.5.

proportionate and dissuasive." I noted, in this regard, that the critical feature of the Draft Decision, and the corrective measure for which it made provision, was that data transfers which were found to be unlawful would cease. That is to say, it is the compelled cessation of the Data Transfers that will right the particular wrongs identified. Against that backdrop, I expressed the view, in the Draft Decision, that the imposition of an administrative fine would not render the DPC's response to the findings of unlawfulness any more effective. Nor did I consider that, in the particular circumstances of this case, or in relation to transfers generally, the imposition of an administrative fine on top of the suspension would have any meaningful dissuasive effect, particularly when set against the consequences said to attach to an order directing the suspension of transfers. I also expressed concern, in the Draft Decision, that the imposition of an administrative fine would be disproportionate, both having regard to the consequences attaching to an order directing suspension of transfers but also because it is ultimately through the Judgment that a series of complex legal issues relating to the Data Transfers have been resolved, and where, in the interim, I considered that the Data Transfers were being effected, in good faith, under and by reference to transfer mechanisms provided for at law.

9.49 I also considered, in the Draft Decision, whether it could be said to be "*appropriate, necessary and proportionate*" to direct Meta Ireland to procure the return and/or deletion of some or of all the personal data that has already been transferred to Meta US. I expressed the view that the making of an order directing the bulk return and/or deletion of all transferred data from an identified point in time would be excessive. In having expressed this view, however, I made it clear that it must (and will) be open to any individual user to exercise the rights conferred on them by Chapter III of the GDPR, in accordance with the law, and to the fullest extent.

9.50 Further to the circulation of the Draft Decision to the CSAs, for the purpose of the Article 60 Process, objections to the conclusions proposed by this Section 9 were raised by the supervisory authorities of Austria, Spain, France and Hamburg (acting on behalf of all German SAs). Those objections expressed disagreement with my view that it would not be appropriate, proportionate or necessary to direct Meta Ireland to procure the return and/or deletion of some or all of the personal data that has already been transferred to Meta US ("the **Deletion or Return Objections**"). They further expressed disagreement with my view that the imposition of an administrative fine would not, in the particular circumstances of this inquiry, be effective, proportionate or dissuasive ("the **Administrative Fine Objections**"). In relation to the Deletion or Return Objections, the EDPB determined as follows:

"1. Preliminary matters related to the scope of the order proposed by the FR and DE SAs

220. As mentioned above, CSAs can propose in their relevant and reasoned objections alternative or additional corrective measures to those envisaged in the Draft Decision, when they consider that the envisaged measures are not 'appropriate, necessary and proportionate' in view of ensuring compliance with the GDPR, taking into account the circumstances of the individual case.

221. In this respect, Article 58(2) GDPR provides a list of corrective powers that can be exercised by SAs to ensure the consistent monitoring and enforcement of the GDPR. These powers are common to all SAs, without prejudice to additional powers provided in national laws. The SAs can therefore decide which measure is the most appropriate and necessary considering the circumstances of the case, but must do so in a way that ensures that the GDPR is fully enforced with all due diligence. Against this background, as the EDPB has previously recalled, a relevant and reasoned objection can also relate to actions other than fines, taking into account the range of powers listed in Article 58(2) GDPR. Thus, CSAs can disagree with the corrective action proposed by the LSA, including when the LSA decides not to impose a specific corrective measure. The CSAs shall then clearly explain the reasons why they consider that a different or additional corrective measure should be imposed, on the basis of a reasoning and conclusion different from the LSA's on the facts collected and the findings established.

222.In this case, the FR SA and the DE SAs clearly explain why, in their view, the IE SA should impose an order regarding the data of EEA users unlawfully transferred to and currently stored in the US. In particular, they refer to the risk to the fundamental rights of data subjects whose data was unlawfully transferred to and is currently processed in the US, subject to disproportionate access by US public authorities and without the possibility to have access to judicial remedies. In the view of the DE SAs and the FR SA, by not imposing such an order, the IE SA fails to draw all the consequences of the unlawfulness of the transfers.

223.Therefore, the EDPB shall assess whether, in light of the objections raised, the envisaged action (in this case, the absence of a measure) included in the draft decision does not comply with the GDPR and whether, consequently, the IE SA needs to include in its final decision, in terms of envisaged actions, also an order regarding the data unlawfully transferred to the

US. In its assessment, the EDPB also takes into consideration Meta IE's submissions, as well as the relevant case law of the CJEU and the objective pursued by the proposed measure.

224.The EDPB underlines that transfers of personal data should only take place when such data will enjoy, in the third country, a level of protection essentially equivalent to that in the EU. In the Draft Decision, the IE SA acknowledges this obligation by proposing a temporary suspension of transfers in accordance with Article 58(2)(j) GDPR in order to 'ensure that the ongoing interferences with the rights of data subjects [...] are brought to an end as soon as possible'. The temporary nature of such order is justified by the IE SA as 'new measures [...] may yet be capable of being developed and implemented by Meta Ireland and/or Meta US to compensate for the deficiencies identified' in the Draft Decision 474. Such deficiencies are found in the 'very clear inadequacies in US law identified by the CJEU' and their impact 'in undermining the protection afforded' to data subjects.

225.In particular, the IE SA finds that US law does not provide an essentially equivalent level of protection to that provided in the EU, that the SCCs relied upon by Meta IE cannot compensate for the inadequate protection and that Meta IE does not have supplementary measures that can compensate for it. The IE SA decides on the suspension of transfers as, in its view, there are no other means to ensure the protection of personal data, in a situation in which the essence of the fundamental right of effective judicial protection of Meta IE's users is not respected.

226.The IE SA takes the view that, if data continued to be transferred to the US, 'the general legislative scheme and policy would be significantly undermined'. This is consistent with the IE SA's findings regarding the breach of Article 46 GDPR due to the lack of supplementary measures that could remedy the identified shortcomings. At the same time, the EDPB notes that, as the FR and DE SAs correctly point out, the order to suspend transfers, as framed in the Draft Decision, only concerns future data transfers and, therefore, it doesn't affect the personal data of EEA users that has already been transferred and is being processed in the US. In this context, the risks identified by the IE SA would continue to be present for the data currently stored in the US despite the corrective measure envisaged by the IE SA. In accordance with the CJEU, SAs shall take appropriate action 'in order to remedy any findings of inadequacy' identified in the context of international data transfers. The CJEU further highlights that the primary responsibility of the SAs to monitor and enforce the application

of the GDPR is 'of particular importance where personal data is transferred to a third country'.

227.Against this background, the DE SAs underline that the cessation of processing in the US, including any storage, is the only measure that can effectively address such risks and, together with the order to suspend the transfers, restore and maintain the level of protection for the personal data of EEA users. The DE SAs also underline that the cessation of the processing could be ordered in the context of, inter alia, a compliance order under Article 58(2)(d) GDPR. Likewise, the FR SA considers that Meta IE should be ordered to bring processing into compliance with the GDPR.

228.The DE SAs also indicate that the return or deletion of the EEA users data stored in the US constitute a 'particularly effective measure' to cease the processing. Likewise, the FR SA indicates the return or deletion of the EEA users' data stored in the US as a measure aimed at ensuring compliance with the GDPR.

229.The EDPB takes note of Meta IE's views in its A65 Submissions and the documents referred therein. In its submissions, Meta IE focuses on the concrete means that the FR SA and the DE SAs consider particularly effective at ensuring compliance with the GDPR, namely the return or deletion of the personal data of EEA users stored in the US. In short, Meta IE states that, from a technical perspective, an order to return personal data would entail the deletion thereof and that the deletion of personal data stored in US data centres would, in turn, entail the deletion of all personal data of EEA users, including personal data stored in the EEA.

230.In this respect, the EDPB underlines that, in accordance with the accountability principle, controllers are responsible for and shall be able to demonstrate compliance with the GDPR. This general principle translates into specific obligations of the controller, including the obligation to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR and that such measures shall be reviewed and updated if necessary. As the EDPB has previously underlined, the right to data protection has an active nature and, in the context of international transfers, it requires exporters and importers to comply in an active and continuous manner by implementing legal, technical and organisational measures that ensure its effectiveness.

231.Therefore, it is within the accountability obligations of controllers to design or, if necessary, update their data processing systems in a way that ensures the lawful processing of personal data under GDPR. This obligation should also apply with regard to systems that require the continuous transferring of personal data to third countries, especially in a case such as the one at hand, in which the CJEU has already declared in two different occasions that the level of protection provided in the US was not essentially equivalent to that in the EU.

232.The EDPB recalls that compliance with the GDPR can be achieved in different manners and, in this particular case, it may not necessarily entail the return or deletion of EEA users' data stored in the US, as other technical solutions could be identified by the controller. For the avoidance of doubt, and given Meta IE's submissions addressing the return and deletion of the EEA users' data stored in the US, the EDPB emphasises that the objections of the FR SA and the DE SAs explicitly request the imposition of an order to bring processing into compliance which, in the case of the DE SAs' objection, is phrased in the form of an order to cease processing. In both cases, the objections mention the return or deletion of the EEA users' data in the US as measures that could achieve such compliance. However, other possible measures are not excluded. This is especially clear in the DE SAs objection, where the DE SAs acknowledge that the cessation of the processing can be implemented by different measures, and only refer to the deletion of personal data as an example thereof.

233.Considering the above, the EDPB will assess whether it should instruct the IE SA to impose an order to Meta IE to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR. If such an order is imposed, it will be the responsibility of Meta IE to identify and implement the appropriate means to bring processing operations into compliance, in accordance with its accountability obligations.

2. Preliminary matters related to the legal basis

234.For the avoidance of doubt, and given Meta IE's arguments regarding the legal basis to impose an order to cease processing as suggested by the DE SAs, the EDPB wishes to address this aspect as a preliminary question.

235.In accordance with Article 58(2)(d) GDPR, an SA can order a controller or processor to bring processing operations into compliance with the provisions of the GDPR, where

appropriate, in a specified manner and within a specific period. The FR SA and the DE SAs explicitly mention this provision as providing for a suitable corrective measure in this case. Meta IE argues that Article 58(2)(d) GDPR 'does not provide the power to require deletion or to require a controller to facilitate the return [...] of data that is being processed by a third party, including its processor'. Meta IE also raises that Article 58(2)(j) empowering SAs to order the suspension of data transfers to a third country does not make any reference to the return or deletion of data already transferred and, in Meta IE's view, 'this omission indicates a preference for the suspension of transfers [...] without affecting personal data transferred prior to the suspension'.

236.As mentioned above, the FR SA and the DE SAs provide in their objections examples of measures that, in this context, appear particularly effective to bring processing into compliance or to cease the processing in the US, namely the return or deletion of the EEA users' data stored in the US. However, the EDPB emphasises that other means to achieve compliance may be available, as recognised by the DE SAs in the objection.

237.In any case, the EDPB wishes to clarify that Article 58 GDPR represents the means for the SAs to perform the tasks enshrined in Article 57 GDPR. In particular, Article 57(1) GDPR provides the obligation of each SA to 'monitor and enforce the application' of the GDPR. In this context, Article 58(2)(d) GDPR clearly sets out the possibility for the SA to order the controller to bring processing into compliance, where appropriate, in a specified manner. In other words, the GDPR provides sufficient flexibility for the SAs to decide, where appropriate, the most appropriate, necessary and proportionate measure to bring processing into compliance.

238.Whenever the legislator considered necessary to specify the content of a type of corrective measure, it did so - this is the case with most of the measures under Article 58(2) GDPR. The fact that the order to comply leaves discretion to the SA on the most appropriate manner to implement it, is a reflection of the intention of the legislator to allow the SAs to decide, where appropriate, on the suitable corrective measure in accordance with the circumstances of the case. Therefore, the EDPB considers that Article 58(2)(d) GDPR cannot be interpreted in such a way that would prevent SAs from specifying the most suitable measure, if the SA considers it appropriate to do so. Such interpretation would render the provision meaningless and would directly contradict settled case law of the CJEU, whereby data protection concepts should be interpreted in light of the fundamental rights enshrined

in the CFR. In addition, the EDPB underlines that the fact that Article 58(2)(j) does not make any reference to the fate of the data already transferred does not prevent SAs from imposing additional corrective measures that will be suitable to the particular circumstances of the case.

239.Therefore, the EDPB agrees with the DE SAs and the FR SA that Article 58(2)(d) GDPR empowers the IE SA to impose in the present case an order to bring processing into compliance with Chapter V, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR as long as this is the appropriate, necessary and proportionate measure in view of ensuring compliance with the GDPR. Contrary to Meta IE's position, the mere fact that such an order may require the controller to procure assistance from their processor to comply is from a legal point of view irrelevant. Otherwise, the effectiveness of an order to bring processing into compliance would depend on the circumstance of whether a processor is involved or not.

240.The DE SAs also consider that the cessation of the processing could also be based on an order to limit processing in accordance with Article 58(2)(f) GDPR, by limiting it with regard to the geographical scope. Meta IE argues that a measure with a 'permanent and irreversible' effect cannot be based on Article 58(2)(f) GDPR. The EDPB notes that Article 58(2)(f) GDPR clearly distinguishes two types of limitations or bans on processing: temporary or definitive. Therefore, an order to cease processing, independently of the nature of the cessation, would clearly be within the powers of the SAs under Article 58(2)(f) GDPR.

241.Finally, with regard to Article 58(2)(g) GDPR, the EDPB takes note of Meta IE's disagreement with the EDPB position in Opinion 39/2021. However, the EDPB upholds its position that Article 58(2)(g) GDPR is a valid legal basis for a supervisory authority to order ex officio the erasure of unlawfully processed personal data in a situation where such request was not submitted by the data subject.

242.In any case, as already explained, the scope of the objections is broader, as the FR SA explicitly requests an order to bring processing into compliance and the DE SAs refer to an order to cease processing, which, in their view, could be imposed on the basis of Article 58(2)(d) GDPR.

243.Given the wording of the objections of the FR SA and the DE SAs, it is clear to the EDPB that in both cases, the aim is to ensure compliance with the GDPR with regard to the

processing of EEA users' data unlawfully transferred and currently stored in the US. Therefore, in this particular case, the EDPB considers that Article 58(2)(d) GDPR provides for the most suitable corrective measure in order to remedy the infringement.

3. The appropriateness of an order to bring processing into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR

244.In the next paragraphs, the EDPB will assess the appropriateness, necessity and proportionality of the order requested by the FR SA and the DE SAs considering the aim pursued, namely, that processing of EEA users' data unlawfully transferred to and currently stored in the US be compliant with the GDPR. Such compliance would be achieved by ceasing the unlawful processing of EEA users' data in the US, including storage, as the DE SAs indicate in their objection.

<u>Appropriateness</u>

245.The EDPB notes that providing for the fate of personal data transferred to a third country, once the relevant transfer(s) is suspended or terminated is not a novelty. In fact, as the DE SAs rightly point out, the former European Commission's SCCs for transfers between controllers and processors included a clause detailing the obligations of the data importer with regard to the personal data already transferred, once the parties agreed to the termination of the data-processing services. This clause has been implemented as an obligation in case of termination of the contract in all modules of the updated SCCs. Likewise, as underlined by the FR SA, Recital 33 of the Privacy Shield decision also provided for the fate of the transferred personal data, in the case of organisations that persistently failed to comply with the Principles. This is especially relevant in the context of a controller-processor relationship where, according to Article 28(1) GDPR, controllers shall only use processors providing sufficient guarantees to comply with the GDPR and ensure the protection of the rights of data subjects.

246.The EDPB takes note of Meta IE's arguments in this respect. The EDPB agrees that the situations envisaged under Recital 33 Privacy Shield, and Clause 12 and 16(d) of the old and current SCCs, respectively, are different from the present case, where the suspension of the

transfers will happen as a consequence of the order imposed by the IE SA. However, those provisions clearly highlight that, once the data importer does not have any legal basis for the processing of the transferred data and/or cannot guarantee compliance with the GDPR, and particularly Chapter V thereof, regardless of the reason, there is a need to provide for the fate of the data already transferred. This is a logical consequence of Article 44 GDPR, which ensures the protection of personal data transferred to third countries.

247.Taking into account the findings of the IE SA in its Draft Decision, and in particular the infringement of the GDPR committed by Meta IE and the risks identified in the Schrems II judgement and confirmed by the IE SA, as well as the elements and reasoning above, the EDPB considers that an order to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR is appropriate, in the present case, in order to remedy non-compliance with the GDPR.

248.In the following section, the EDPB will analyse whether the order is also necessary and proportionate taking into account the circumstances of the specific case.

<u>Necessity and proportionality</u>

249.In the Draft Decision, the IE SA considers that an order to return or delete personal data already transferred 'would be excessive' and that it is 'open to any individual user to exercise the rights' under the GDPR 'to the fullest extent'. The FR SA and the DE SAs disagree with the IE SA and consider that the processing of personal data unlawfully transferred to and currently stored in the US needs to be brought into compliance with the GDPR, as explained above, and refer to some concrete measures that could achieve such compliance. In its submissions, Meta IE focuses heavily on those concrete measures and argues that the return of the data is not appropriate and the deletion is neither appropriate, given its 'significant and permanent adverse effects', nor necessary, as the dissuasive effect is already achieved with the order to suspend transfers, nor proportionate, in light of the temporary nature of the order to suspend transfers and the irreversible character of the order to delete data. In its submissions, Meta IE does not address other possible means to bring processing into compliance.

250.As a preliminary remark, the EDPB underlines that the possibility for data subjects to exercise their rights under the GDPR does not prevent SAs from adopting appropriate

corrective measures to remedy an infringement. The EDPB fundamentally disagrees with a position that, in practice, would entail entrusting the enforcement of the GDPR to individual actions without requiring controllers to remedy the infringements identified. This position, in the view of the EDPB, would undermine the effective application of one of the two overall objectives of the GDPR, namely the protection of the 'fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'

251.As the EDPB has previously recalled, supervisory authorities are required to react appropriately to remedy infringements of the GDPR, in accordance with the means provided to them by Article 58(2) GDPR. Corrective measures should be applied inasmuch as they are appropriate, necessary and proportionate in accordance with the circumstances of the individual case. This highlights the need for the corrective measures and any exercise of powers by supervisory authorities to be tailored to the specific case. This is in line with settled case law of the CJEU, according to which measures shall not exceed the limits of what is appropriate and necessary in order to achieve the objectives legitimately pursued; where there is a choice between several appropriate measures, recourse must be had to the least onerous and the disadvantages caused must not be disproportionate to the aims pursued.

252.The EDPB has consistently referred to the need to ensure, when choosing the appropriate corrective measure, that such measure is necessary to enforce the GDPR and achieve the protection of the data subjects with regard to the processing of their personal data. Thus, when there is a choice between several appropriate measures, the principle of proportionality requires that the least onerous measure be chosen and that it does not create disproportionate disadvantages in relation to the aim pursued.

253.The EDPB takes note of the elements raised by the objections of the FR SA and DE SAs to justify the need for imposing an order with regard to EEA users' personal data unlawfully transferred to and currently stored in the US. In particular, the FR SA refers to the 'significant risks' of infringement of the privacy of individuals due to access to data by US public authorities, as identified in the Schrems II judgement and in the Draft Decision. The DE SAs also refer to the risk of 'disproportionate access by US authorities' and the lack of effective legal remedies, which, in their view, 'results in a permanent high risk to the fundamental rights and freedoms of the data subjects that is not remedied' by the action envisaged in the Draft Decision.

254.As mentioned in paragraph 224 above, in the Draft Decision the IE SA considers that the 'very clear inadequacies in US law' undermine the protection afforded to data subjects and the essence of their fundamental right to effective judicial protection is not respected. Considering these findings, the FR SA and the DE SAs argue that the processing of EEA users' data unlawfully transferred to and currently stored in the US needs to be brought into compliance with the GDPR. The IE SA does not address the FR SA and DE SAs' arguments and concerns on the risks to which the data already transferred to and currently stored in the US are subject.

255.In this respect, the EDPB considers that the objective pursued by the order to bring processing operations into compliance is a legitimate one. The EDPB takes note of Meta IE's argument that the practical risk of interference with EEA users data transferred to the US 'has always been extremely limited' and, in the case of EEA users' data previously transferred to the US, the potential risk is 'even more limited'. However, the EDPB is not swayed by this argument, as analysed above.

256.The EDPB also takes note of Meta IE's arguments, whereby an order to delete will be unnecessary in terms of dissuasiveness and disproportionate due to the 'very significant additional irreparable harm' that it would cause. However, as stated above, the deletion of the personal data of EEA users stored in the US is only one of the possible ways to bring processing into compliance. Whether such measure would also entail the deletion of all personal data of EEA users would be, in any case, a consequence of the architecture of the system chosen by Meta IE to provide the Facebook service. Consequently, it is the controller's responsibility to identify and implement the appropriate measures to bring processing of EEA users data unlawfully transferred to and currently stored in the US into compliance with the GDPR.

257.The EDPB recalls that, when assessing whether a specific corrective measure attains the objective pursued, several factors need to be taken into consideration, in addition to the dissuasiveness of the measure, namely, its ability to remedy an infringement and restore the level of protection of the GDPR. In the present case, the above considerations demonstrate that an order to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, is necessary in order to achieve the aim pursued, namely

that processing of EEA users' data unlawfully transferred to and currently stored in the US be compliant with the GDPR.

258.With regard to the proportionality of the proposed order, Recital 129 GDPR provides that consideration should be given to ensuring that measures chosen to remedy an infringement do not create 'superfluous costs' and 'excessive inconveniences' for the persons concerned in light of the objective pursued. In the present case, the EDPB understands the need, on the one hand, to ensure that data subjects' personal data are processed in accordance with the GDPR and not subject to disproportionate risks and, on the other hand, to ensure the integrity of such data and the rights of the data subjects.

259.The EDPB has previously recalled that the seriousness of the infringement is an important element to take into account when assessing the proportionality of a corrective measure, as Recital 148 GDPR demonstrates. In this case, the IE SA underlines, following the Schrems II judgement, that the essence of the fundamental right to a judicial remedy is not respected with regard to data subjects whose data is transferred to the US. This contributes to considering the breach at stake as a particularly serious infringement, as concluded in paragraph 99 of this Binding Decision.

260.The EDPB takes note of Meta IE's submissions where it argues that, given the inherent interconnectedness of the Facebook service's social graph, 'any order to "cease the processing" of Meta Ireland User Data in the US [...] would in effect be an order to delete such data'.

261.The EDPB considers, however, that the order proposed by the FR SA and the DE SAs does not impose a specific manner for the controller to comply with it. On the contrary, it gives enough room of manoeuvre to Meta IE to identify the most suitable manner to implement the order, in accordance with its accountability obligations. Taking this into consideration, the EDPB is of the view that this is the least onerous measure possible, as the controller will be the one ultimately making the choice of the specific manner to comply with the order. It goes without saying that, when deciding on the means to comply and when implementing the necessary steps to do so, the rights of data subjects must be respected, as it stems from Article 24(1) GDPR.

262.Therefore, the EDPB is of the view that the proposed order is proportionate to the aim pursued, since it is the least onerous measure possible and it does not create disproportionate disadvantages to the aim pursued.

Conclusion

263.On the basis of the conclusions above, the EDPB considers that an order to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR is appropriate, necessary and proportionate to the circumstances of the case.

264.With regard to the period for compliance with such order, the EDPB takes note of the FR SA's request that such period shall 'allow data subjects to exercise their rights'. The FR SA does not specify a concrete timeframe. The DE SAs consider that the order should be complied with 'within a reasonable period of time, which shall not exceed 6 months after the termination of this cooperation procedure'.

265.On one hand, the EDPB understands that compliance with the order may require technical and organisational adjustments on the side of Meta IE. On the other hand, the EDPB notes that the compliance period proposed by the DE SAs is considerably longer than the one envisaged in the Draft Decision regarding the transfer suspension order. Therefore, the EDPB considers that a period of 6 months, as requested by the DE SAs, provides sufficient time for Meta IE to identify and implement the specific measures to bring processing operations into compliance.

266.The order to bring processing operations into compliance with Chapter V GDPR should take effect on the date of notification of the IE SA's final decision to Meta IE.

267.On the basis of the above considerations, the EDPB instructs the IE SA to include in its final decision an order for Meta IE to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, within 6 months following the date of notification of the IE SA's final decision to Meta IE.

9.51 Accordingly, and as directed by the EDPB further to the Article 65 Decision, I have included, in Section 10, below, an order requiring Meta Ireland to bring processing operations into

compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, within the period of 6 (six) months from the date on which this Decision is notified to Meta Ireland ("the **Cessation Order**"). I note, in this regard, that neither the CSAs (by way of the Deletion or Return Objections or otherwise) nor the EDPB expressed disagreement with my view, set out at paragraph 9.46 above, that "*new measures, not currently in operation, may yet be capable of being developed and implemented by Meta Ireland and/or Meta US to compensate for the deficiencies identified herein*". While that view was expressed in the context of the suspension order that was proposed by the DPC in the Draft Decision (and which is reflected in Section 10, below), it applies equally to the Cessation Order. Accordingly, and for the sake of clarity and legal certainty, the orders specified in Section 10, below, will remain effective unless and until the matters giving rise to the finding of infringement of Article 46(1) GDPR have been resolved, including by way of new measures, not currently in operation, such as the possible future adoption of a relevant adequacy decision by the European Commission pursuant to Article 45 GDPR.

9.52 For the sake of completeness, I note that Meta Ireland indicated[210] its expectation that, as regards the deadline for compliance with the Cessation Order, the DPC would "*word*" the deadline for compliance in similar terms to the deadline applicable to the suspension order that was proposed by the DPC in the Draft Decision (and which is reflected in Section 10, below). The applicable enforcement period is a period of 12 weeks, which commences after the expiry of specified statutory limitation periods. The EDPB gave consideration, during the Article 65 Process, to the possibility of formulating the timeline for compliance with the Cessation Order in a manner which aligned to the approach taken by the DPC, as regards the date on which the timeline for compliance would commence. The EDPB ultimately decided against this approach and instead determined that the applicable deadline for compliance (with Cessation Order) should commence immediately upon the notification of this Decision to Meta Ireland. In circumstances where the Article 65 Decision is binding upon the DPC (and all CSAs), it is not open to me to take account of Meta Ireland's request to reformulate the date of commencement in respect of the Cessation Order compliance period.

9.53 In relation to the Administrative Fine Objections that were raised by the CSAs during the Article 60 GDPR consultation period, the EDPB determined as follows:

[210] The Final Submissions, Section 6, paragraph 6.2

78. In accordance with Article 65(1)(a) GDPR, the EDPB shall take a binding decision concerning all the matters which are the subject of the relevant and reasoned objections, in particular whether the envisaged action in the Draft Decision with regard to the controller complies with the GDPR. The EDPB considers that the objections found to be relevant and reasoned in this section, raised by the AT SA, DE SAs, ES SA, and FR SA, requested the IE SA to exercise its power to impose an administrative fine and propose the imposition of corrective measures in addition to the ones proposed in the LSA's Draft Decision. When assessing the merits of the objection raised, the EDPB also takes into account Meta IE's position on the objection and its submissions.

79. The EDPB is therefore required to assess whether the IE SA's proposal in the Draft Decision not to impose an administrative fine pursuant to Article 58(2)(i) GDPR for the infringement by Meta IE of Article 46(1) GDPR is in accordance with the GDPR. Meta IE's position 'is that the DPC exercised its discretion properly in the Draft Decision in deciding not to impose an administrative fine on Meta Ireland'.

80. The EDPB recalls that the consistency mechanism may also be used to promote a consistent application of administrative fines, as highlighted by Recital 150 GDPR. This is the case, among others, in situations where the relevant and reasoned objections challenge the decision by the LSA not to propose the imposition of an administrative fine (and propose the imposition of additional corrective measures) and in situations where a relevant and reasoned objection challenges the elements relied upon by the LSA to calculate the amount of the fine.

81. Meta IE considers that the LSA has sole discretion to determine the appropriate corrective measure and that Article 65(1) GDPR does not confer competence to the EDPB to instruct the LSA to impose an administrative fine. According to Meta IE, it would be contrary to Articles 4(24) and 58(2)(i) GDPR 'for the CSAs and/or the EDPB to seek to substitute their own views of the corrective measures for those of the [IE SA]'. In this respect, the EDPB highlights that the views of Meta IE amount to a misunderstanding of the GDPR one-stop-shop mechanism and of the shared competences of the CSAs. The GDPR requires supervisory authorities to cooperate pursuant to Article 60 GDPR to achieve a consistent interpretation of the Regulation. Pursuant to Articles 56(1) and 60(1) GDPR, in cross-border cases, the LSA shall cooperate with the other CSAs in an endeavour to reach consensus. Considering that in such cases the final decision of the LSA has cross-border effects (potentially across the

entire EEA), consensus should also be reached with regard to the appropriate corrective measures. While the LSA is the authority that can ultimately exercise the corrective powers listed in Article 58(2) GDPR, this cannot diminish the role of the CSAs within the cooperation procedure or the role of the EDPB in the consistency procedure.

82. The CSAs may raise an objection on the existing or missing corrective measures in the Draft Decision when, in their views, the envisaged action does not comply with the GDPR, in which case they should indicate which action they believe would be appropriate for the LSA to include taking into consideration the risks at stake. The dispute resolution competence of the EDPB covers 'all the matters which are the subject of the relevant and reasoned objections'. Therefore, in case of disagreement, the consistency mechanism may also be used to promote a consistent application by the supervisory authorities of their corrective powers, taking into account the range of powers listed in Article 58(2) GDPR, when a relevant and reasoned objection questions the action(s) envisaged by the Draft Decision vis-a-vis the controller/processor, or the absence thereof.

83. In accordance with Article 58(2) GDPR, the imposition of administrative fines pursuant to Article 83 GDPR is only one of the corrective powers vested with the SAs. The wording 'in addition to, or instead of' in Article 58(2)(i) makes it clear that different corrective measures can be combined, as long as the requirements of Article 83 GDPR are met. Nevertheless, it should be borne in mind that, as highlighted by the WP29, 'Administrative fines are a central element in the new enforcement regime introduced by the Regulation, being a powerful part of the enforcement toolbox of the supervisory authorities together with the other measures provided by article 58 [GDPR]'.

84. The EDPB takes note of Meta IE's views that 'the GDPR does not mandate the imposition of fines in any particular circumstances'. The EDPB concurs that the decision to impose an administrative fine needs to be taken on a case-by-case basis, in light of the circumstances of each individual case, as mentioned in Recital 129 GDPR and Article 58(2)(i) GDPR. It is clear from the wording of Article 83(2) GDPR that the factors listed thereunder are meant not only to enable the SAs to calculate the amount of the administrative fine in each individual case, but also to decide 'whether to impose an administrative fine' in the first place. Thus, the EDPB fully agrees with the DE SAs' view that the criteria set out in Article 83(2) GDPR 'influence the discretion to issue an administrative fine'. Where a supervisory

authority decides to impose an administrative fine on the basis of Article 83(2) GDPR, it should also make sure that the requirements of Article 83(1) GDPR are fulfilled.

85. In light of the above, the EDPB will first examine the application of the relevant criteria under Article 83(2) GDPR. The main elements to be taken into account when assessing the application of Article 83(2) GDPR were already established in the EDPB Guidelines on Administrative Fines, and the complementary EDPB Guidelines on the calculation of fines under the GDPR.

86. In this regard, the EDPB notes that in the Draft Decision the IE SA mentions that it has 'carefully considered the criteria set out in GDPR Article 83(2)(a)-(k)' 194 without providing further details. In the context of exchanges between the EDPB Secretariat and the IE SA in the context of the analysis of the completeness of the file, aimed at ensuring that all relevant elements and documents (e.g. concerning the IE SA's position on this matter) were available to the EDPB to support its decision-making, the IE SA confirmed that no further documentation on its consideration of the criteria had to be added as all documents relating to this issue were already included in the file transmitted to the Secretariat.

87. On the basis of the available and relevant documents and taking into account the relevant and reasoned objections raised, the EDPB proceeds with an assessment of the criteria under Article 83(2) GDPR as applicable to the case at hand. As further described below, the overall analysis of the relevant factors listed in Article 83(2) GDPR demonstrates the need to impose an administrative fine for the identified infringement of Article 46(1) GDPR.

88. Article 83(2) GDPR 'provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine': as explained in the EDPB Guidelines on Administrative Fines, this does not consist in 'a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case', and the 'conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice'.

<u>On the nature, gravity and duration of the infringement (Article 83(2)(a) GDPR)</u>

89. Pursuant to Article 83(2)(a) GDPR, when assessing the nature, gravity and duration of the infringement, the SA shall give due regard to the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage they suffered.

90. With regard to the nature and gravity of the infringement, Meta IE argues that account has to be taken of the 'highly unusual circumstances of the alleged infringement of Article 46(1) GDPR' and in particular that 'Meta Ireland has always made the Meta Ireland Data Transfers in good faith'. The EDPB considers that this argument relates to Article 83(2)(b) GDPR rather than to Article 83(2)(a) GDPR and will examine it below.

91. In its Draft Decision, when assessing the imposition of corrective measures for the established infringement of Article 46(1) GDPR, the IE SA underlines that 'the deficiencies in US law identified by the CJEU have not been addressed by the SCCs or supplemental measures, that a derogation under GDPR Article 49(1) is not available to Meta Ireland, and that the Data Transfers have been found to give rise to a breach of the essence of one or more fundamental rights'. In this regard, the EDPB highlights that an infringement giving rise to a breach of the essence of a fundamental right shall be considered as a grave one. In addition, the EDPB agrees with the arguments put forward by the AT SA, DE SAs, ES SA and FR SA, which consider that the infringement is particularly serious. More specifically, according to the ES SA, the FB International Transfers 'are not occasional or sporadic' but 'systematic, mass, repetitive and continuous in nature'. Likewise, the AT SA considers that Meta IE has been substantially and continuously violating data subject rights for several years. In the FR SA's view, the breach is particularly serious in terms of the data subjects' privacy. The DE SAs refer to the large number of data subjects concerned, the long period of the infringement and the scope of the processing.

92. Regarding the nature, scope and purpose of the processing concerned, the EDPB takes note of Meta IE's description of the processing as being 'simply the transfer of Meta Ireland User Data by Meta Ireland to its processor, MPI, in the US for the purpose of supporting Meta Ireland in its provision of the Facebook Service to Meta Ireland Users'. Specifically concerning the scope, Meta IE considers that the scale of the processing is not a relevant factor to assess whether to impose an administrative fine. Notwithstanding, the EDPB finds that Article 83(2)(a) GDPR entails that the scope or scale of the processing is a relevant factor when deciding whether to impose an administrative fine. More particularly, the EDPB

recalls that the processing at stake has a particularly large scope and agrees with the DE SAs' view that the 'context of data processing extents to huge amounts of social interactions generated by these data subjects each and every day for the past and ongoing'. This is confirmed by the IE SA itself, which describes the transfers as 'systematic, bulk, repetitive and ongoing' throughout Section 8 of the Draft Decision.

93. As to the number of data subjects affected, the EDPB considers the DE SAs' observation that Meta IE has '309 million daily active users in Europe' and that therefore 'a large share of the entire population of the European Union is directly affected by the non-compliance' of Meta IE' is particularly relevant. The same is supported by the FR and AT SAs, which also correctly observe that a 'particularly massive volume of data' is at stake 'since the Facebook service has millions of users in the European Union' and that 'Meta is the provider of the biggest global social media network with an enormous number of users within the European Union and thus affected persons'.

94. Meta IE does not dispute the fact that 'a large number of data subjects have been involved' as the Facebook Service is used by a very high number of users. In its submissions on the Preliminary Draft Decision, Meta IE itself explains that 'Since its introduction in 2004, the Facebook Service has become an extremely popular and well-known online global communication and content sharing service, used by approximately 2.85 billion users globally every month to share and access information and connect with others around the world. This includes more than 255 million individual users in the EU / EEA'. However, according to Meta IE, 'the fact that personal data of a large number of data subjects have been involved in the Meta Ireland Data Transfers does not equate to a large number of data subjects being "affected" for the purpose of Article 83(1)(a) GDPR'. It further argues that 'There was always only an extremely limited practical risk of alleged interference with Meta Ireland Users' data protection and redress rights as a result of the Meta Ireland Data Transfer, and any such risk only involved an extremely limited number of Meta Ireland Users'.

95. The EDPB cannot agree with Meta IE's arguments. As explained in the EDPB Guidelines on calculation of fines, the number of data subjects affected should mean 'concretely but also potentially affected'. In other words, 'affected' data subjects are not only data subjects whose accounts have been subject to access requests, but also data subjects whose accounts could have been subject to access requests. The EDPB recalls that, at the time of

this dispute resolution procedure, the infringement is still ongoing, which means that the personal data of Facebook users is transferred to and processed in the US without appropriate safeguards, as required by Article 46(1) GDPR.

96. Therefore, the EDPB concludes that a very high number of data subjects is affected and this already high number can keep increasing until the infringement is effectively brought to an end.

97. Regarding the duration of the infringement, the DE SAs and AT SA stress that it has been ongoing for several years, which they see as an aggravating factor. According to the AT SA, the duration of the infringement resulted in data subjects' rights being 'substantially and continuously violated'. The DE SAs point out that 'the duration of the infringement for the data subjects extents to even before GDPR with the previous regimen with the same legal obligations for controllers'. The DE SAs further highlight that 'the data processing of the undertaking is under scrutiny of supervisory authorities since about ten years'. Meta IE responds to this by stressing that the inquiry only concerns the period since the GDPR became applicable.

98. The EDPB takes note of the IE SA's explanation that the purpose of the Draft Decision is 'to consider whether Meta Ireland is acting [...] compatibly with GDPR Article 46(1), in making transfers [...] of personal data relating [...] to Meta US pursuant to standard contractual clauses [...], following the judgment of the Court of Justice of the European Union ("the CJEU"), delivered on 16 July 2020, in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems'. The EDPB also notes that no CSA raised objections concerning the temporal scope of the Draft Decision. Therefore, the starting point of the infringement at stake should be determined on the basis of the description made in the Draft Decision only, i.e. from 16 July 2020 (date of the adoption of the Schrems II judgment). The EDPB considers that this duration of infringement is significant and has to be taken into account when deciding whether an administrative fine should be imposed.

99. As a conclusion, the EDPB considers that, taking into account the nature and scope of the processing, as well as the very high number of data subjects affected, Meta IE committed an infringement of significant nature, gravity and duration. Therefore, this

criterion has to be taken into account when deciding whether an administrative fine should be imposed.

On the intentional or negligent character of the infringement (Article 83(2)(b) GDPR)

100. Article 83(2) GDPR mentions, among the factors to be taken into account when deciding the imposition and amount of an administrative fine, 'the intentional or negligent character of the infringement'. Recital 148 GDPR also requires that due regard be given to the 'intentional character of the infringement'.

101. Meta IE agrees with the IE SA's conclusion that the FB International Transfers were made by Meta IE in good faith because it has implemented supplemental measures in addition to the 2021 SCCs, and has believed that, in the alternative, was entitled to rely on Article 49 GDPR. Meta IE argues that the IE SA's finding that Meta IE made the FB International transfers in good faith is a factual finding on the basis of which the EDPB must make its decision and which is not the subject of any objection by the CSAs.

102. The EDPB cannot agree with Meta IE's arguments. The IE SA found that Meta IE has relied on SCCs and, alternatively on the derogations under Article 49 GDPR and concluded that Meta IE acted 'in good faith'. The EDPB notes that this conclusion is, contrary to what Meta IE argues, the subject of the objections and hence of the dispute. As previously explained in Section 4.2 of this Binding Decision, all the objections raised by CSAs on the matter of the imposition of an administrative fine express views on the intentionality of the infringement and disagree with the assessment that Meta IE acted in good faith when carrying out the FB International Transfers. More specifically, the FR SA argued the infringement had an 'intentional character' as it was 'committed deliberately by the company'. The ES SA also mentions that Meta IE 'has been in breach of the GDPR despite its knowledge [since the Schrems II judgment]' that the FB International Transfers would trigger a breach of the GDPR. The DE SAs also argue that Meta IE acted intentionally or at least - as argued by the AT SA - with dolus eventualis. These statements included in the objections amount to disagreements with the finding that Meta IE acted in good faith in carrying out the FB International Transfers.

103. As already clarified in the EDPB Guidelines on Administrative Fines, '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'. In other words, the EDPB Guidelines on calculation of fines confirm that there are two cumulative elements on the basis of which an infringement can be considered intentional: the knowledge of the breach and the wilfulness in relation to such act. On the other hand, an infringement is 'unintentional' when there was a breach of the duty of care, without having intentionally caused the infringement. The EDPB also recalls that the intentional or negligent character of the infringement 'should be assessed taking into account the objective elements of conduct gathered from the facts of the case' and that 'depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence'.

104. The EDPB notes and agrees with the DE SAs' observation that Meta IE has been 'under scrutiny of supervisory authorities since about ten years': the two landmark judgments issued by the CJEU in 2015 and in 2020 were also issued in cases concerning this same company. Indeed, as recalled by the IE SA in the Draft Decision, the original complaint against Meta IE which contended that the transfer of personal data by Meta IE to Meta Platforms, Inc., in reliance on the 'Safe Harbor' adequacy decision, was unlawful and which led to judicial proceedings in Ireland and then to the preliminary ruling of the CJEU in 2015 in the case C-362/14, Schrems v Data Protection Commissioner ('Schrems I judgment'), was filed by Schrems with the IE SA on 25 June 2013. The Schrems II Judgment, as previously mentioned, was handed down by the CJEU on 16 July 2020. Following the IE SA Preliminary Draft Decision of 28 August 2020 and the opening of inquiry IN 20-8-1, Meta IE commenced judicial proceedings against the IE SA.

106. The EDPB recalls the IE SA's conclusion that the 2021 SCCs Meta IE relied upon to carry out the FB International Transfers could not remedy the inadequate protection afforded by US law. The EDPB also notes that the IE SA examined in detail the question of whether Meta IE has put in place supplementary measures that could address the insufficiencies of the protection provided by US Law and its conclusion that this is not the case.

107. As explained by the EDPB in its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (hereinafter 'EDPB Recommendations on Supplementary Measures'), when assessing third countries and identifying appropriate supplementary measures, controllers should assess if there is anything in the law and/or practices in force of the third country that may

impinge on the effectiveness of the appropriate safeguards of the transfer tools that they are relying on. In this regard, the EDPB notes that, according to Meta IE's assessment, 'the level of protection required by EU law is provided for by relevant US law and practice' and that Meta IE implemented supplementary measures in addition to the 2021 SCCS in order to 'further ensure that an adequate level of protection continues to apply to User Data transferred from FIL to FB, Inc'. In other words, Meta IE has implemented supplementary measures on the basis of an assessment which concluded that there was no need for such measures, since, in Meta IE's view, the relevant US law and practice were already providing a level of protection equivalent to the one provided under EU law.

108. Moreover, the EDPB highlights the IE SA's concern that Meta IE's submissions 'seem to simply ignore the ruling of the CJEU' and 'that Meta Ireland is seeking to promote a lower standard for the objective of SCCs and supplemental measures than is permitted by the Judgment and the GDPR'. More specifically, the IE SA notes that Meta IE 'seems to identify its own test for determining suitability of supplemental measures by lowering the standard to include measures that can "address" or "mitigate" any "relevant remaining" inadequacies in the protections offered by US law and practice and the SCCs', and concludes in the Draft Decision that 'Meta Ireland does not have in place any supplemental measures which would compensate for the inadequate protection provided by US law'.

105. In addition, the EDPB takes note of Section 7 of the Draft Decision, where the IE SA first sets out the framework of its assessment and then examines in detail the lawfulness of the transfers, by following the terms of Article 46(1) GDPR as reflected by the Schrems II Judgment. The EDPB also takes note of the IE SA's assessment in Section 8 of the Draft Decision and the conclusion that it is 'not open to Meta Ireland to rely on the derogations at Article 49(1) (or any of them) to justify the systematic, bulk, repetitive and ongoing transfers of its users' data from the EU to the US'.

109. Considering the detailed assessment of the US legal system by the CJEU in the Schrems II judgment, the series of steps to follow, sources of information and examples of supplementary measures provided in the EDPB Recommendations on Supplementary Measures', as well as the IE SA's findings in the Preliminary Draft Decision and Revised Preliminary Draft Decision which were shared with Meta IE prior to the Draft Decision, the EDPB takes the view that Meta IE could not have been unaware of the fact that the FB International Transfers could be considered in violation of Article 46(1) GDPR.

110. In light of the above, the EDPB concludes that there are sufficient indications that Meta IE committed the infringement of Article 46(1) GDPR knowingly.

111. Additionally, with respect to the finding of the IE SA that reliance on Article 49 GDPR was not open to Meta IE for the purpose of carrying out the FB International Transfers, the EDPB is of the view that at the very least Meta IE could not have been unaware of the guidance of the EDPB and of the findings of the CJEU that the derogations cannot be relied upon for systematic and massive transfers and have to be strictly construed.

112. As regards the 'wilfulness' component of intent, the EDPB recalls that the CJEU has established a high threshold in order to consider an act intentional. The EDPB has previously recalled that even in criminal proceedings, the CJEU has acknowledged the existence of 'serious negligence', rather than 'intentionality' when 'the person responsible commits a patent breach of the duty of care which he should have and could have complied with in view of his attributes, knowledge, abilities and individual situation'. Although a company for which the processing of personal data is at the core of its business activities is expected to have sufficient measures in place for the safeguard of personal data and for the thorough understanding of its duties in this regard, this does not per se demonstrate the wilfulness of an infringement. In this regard, the EDPB notes that Meta IE has taken steps in order to achieve compliance with Chapter V of the GDPR following the Schrems II judgment, but these steps were not sufficient to achieve compliance as established by the Draft Decision. Consequently, the EDPB takes the view that, on the basis of the objective elements in the case file, 'wilfulness' on the side of Meta IE is not fully demonstrated.

113. Nevertheless, the EDPB stresses that Meta IE's position that the relevant US law and practice were already providing a level of protection equivalent to the one provided under EU law in spite of the Schrems II judgment, the lower standard applied by Meta IE when implementing the SCCs and supplementary measures, as well as the subsequent failure to implement supplementary measures that were aimed to compensate (and could compensate) for the inadequate protection provided by US law (rather than address or mitigate 'any relevant remaining inadequacies in the protection afforded by US law and practice', as argued by Meta IE), indicate a very high degree of negligence on the side of Meta IE. As the IE SA correctly recalls, 'the terms "mitigate" and "address" cannot be found in either the Judgment or the GDPR'. In addition, the EDPB notes that Meta IE contests the IE SA's interpretation of the Schrems II judgment and of the test for determining suitability

of supplementary measures not only in its submissions on the Preliminary Draft Decision, but also in its submissions on the Revised Preliminary Draft Decision. Therefore, it appears that, by not applying the correct test for determining the suitability of supplementary measures in spite of the clear requirement that the appropriate safeguards to be taken by the controller must 'compensate for' the lack of data protection in the third country, Meta IE breached its duty of care and acted at least with the highest degree of negligence.

114. This is the case also in light of the arguments brought by the AT SA and DE SAs that Meta IE has acted at least with conditional intent (dolus eventualis) 'since it must have seriously considered a violation of Chapter V GDPR when carrying out data transfers'. The EDPB has previously explained that 'Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence'.

115. In light of the above, the EDPB takes the view that Meta IE committed the infringement at least with the highest degree of negligence and this has to be taken into account when deciding whether an administrative fine should be imposed.

<u>On the degree of responsibility of the controller taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 (Article 83(2)(d) GDPR)</u>

116. The EDPB recalls that, pursuant to Article 83(2)(d) GDPR, the degree of responsibility of the controller or processor will have to be assessed, taking into account measures implemented by them to meet the requirements of data protection by design and by default (Article 25 GDPR) and of security of processing (Article 32 GDPR). More specifically, the EDPB has explained that 'the question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation'. In addition, the residual risk for the freedoms and rights of the data subjects, the impairment caused to the data subjects and the damage persisting after the adoption of the measures by the controller as well as the degree of robustness of the measures adopted pursuant to Articles 25 and 32 GDPR must be assessed.

117. The EDPB has also explained that, given the increased level of accountability under the GDPR, it is likely that this factor will be considered either an aggravating or a neutral one.

Only in exceptional circumstances, where the controller or processor has gone above and beyond the obligations imposed upon them, will this be considered a mitigating factor.

118. Meta IE argues that 'the issue regarding EU-US data transfers is fundamentally one of a "conflict of laws" between the EU and the US' and that it has conducted all appropriate assessments, maintained all documentation and taken all steps available to it as soon as possible, such as entering into the 2021 SCCs.

119. The EDPB considers that these arguments have no bearing on the degree of responsibility of Meta IE in the present case.

120. It is clear from Article 25(1) GDPR that the controller is under an obligation, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. In addition, Article 32(1) GDPR lays down an obligation for the controller, by taking into account a number of factors, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons. Article 32(2) GDPR further specifies that, in assessing the level of security, account shall be taken in particular of the risks that are presented by processing, in particular from [...] unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

121. In this regard, the EDPB recalls that the IE SA carries out a detailed assessment of whether Meta IE implemented supplementary measures that could address the inadequate protection provided by US law. More specifically, the IE SA analyses the organisational, technical and legal measures implemented by Meta IE and concludes that these measures cannot, 'whether viewed in isolation, or in tandem with the 2021 SCCs and the full suite of measures outlined in the ROS', compensate for the deficiencies identified in US law and cannot provide essentially equivalent protection to that available under EU law.

122. This results in a high residual risk for the rights and freedoms of the data subjects concerned, because, as highlighted by the IE SA, data subjects are still not protected against

702 FISA DOWNSTREAM (PRISM) requests and Meta US would still be required to disclose its users' personal data, if requested by the US Government.

123. It is relevant also to recall that the EDPB Recommendations 1/2020 clarified that controllers may have to apply some or all of the measures described therein even irrespective of the level of protection provided for by the laws applicable to the data importer because they need to comply with Articles 25 and 32 GDPR in the concrete circumstances of the transfers.

124. Against this background, the EDPB recalls the DE SAs view that, considering the amount of data processed, 'the responsibility may have been heightened above average'. The EDPB also finds particularly relevant the FR SA's observation that the Facebook social network occupies an 'inescapable place in France' since it 'dominates by far the social media market' and, due to its dominant position, generates important 'network effects'. The EDPB considers that this is the case not only in France, but in the EEA in general. In addition, the Facebook service is provided to many users who do not necessarily have legal or technical knowledge. These users rely on the information published by Meta IE and therefore would reasonably expect that their personal data is protected when it is transferred to the US. Finally, the EDPB concurs with the FR SA's view that 'in parallel with its traditional function of maintaining and developing interpersonal relationships, this social network also occupies an increasingly larger role in areas as diverse as access to information, public debate or even civil security'.

125. In light of the above considerations, the EDPB takes the view that there are enough elements in the analysis of this factor which confirm Meta IE's high degree of responsibility. Therefore, this factor has be taken into account when deciding whether to impose an administrative fine.

<u>Any relevant previous infringements by the controller (Article 83(2)(e) GDPR)</u>

126. The EDPB recalls that, according to Article 83(2)(e) GDPR and Recital 148 GDPR, any relevant previous infringements committed by the controller or processor are to given due regard when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine. In addition, the absence of any previous infringements cannot be considered a mitigating factor, as compliance with the GDPR is the norm and if there are no previous infringements, this factor can be regarded as neutral. The EDPB has already

explained that prior infringements are relevant as they might provide an indication about the controller's general attitude towards the observance of the GDPR and that recent infringements under the GDPR have more significance than infringements that have taken place long time ago.

127. In this regard, the EDPB notes the AT SA's remark that 'it is not the first case where the DPC has established a violation of the GDPR by Meta Ireland'. The AT SA Objection does not make reference to specific cases where the IE SA has established a violation of the GDPR by Meta IE, but it is possible to recall in particular the IE SA's decisions adopted following EDPB Binding Decisions 2/2022 of 28 July 2022 and 3/2022 and 4/2022 of 5 December 2022 where the IE SA found that Meta IE breached the GDPR. The EDPB recalls that at the time when the Draft Decision was circulated to the CSAs, the IE SA's final decision in these cases had not yet been adopted. Therefore, nothing arises to be taken into account here when deciding whether an administrative fine should be imposed on Meta IE.

<u>On the categories of personal data affected by the infringement (Article 83(2)(g) GDPR)</u>

128. Concerning the requirement to take account of the categories of personal data affected under Article 83(2)(g) GDPR, the EDPB recalls that the GDPR clearly highlights the types of data that deserve special protection and therefore a stricter response in terms of fines. The EDPB has already explained that categories of personal data deserving a stricter response in terms of fines include at the very least, the types of data covered by Articles 9 and 10 GDPR, and data outside the scope of these Articles the dissemination of which causes immediate damages or distress to the data subject, such as location data, data on private communication, national identification numbers, or financial data.

129. The EDPB takes note of the large number of categories of personal data transferred to the US, as outlined in the Draft Decision. More specifically, Part A of Appendix 1 to the Meta US's Data Transfer and Processing Agreement of 25 May 2018 mentions: 'the personal data generated, shared and uploaded by or about individuals who visit, access, use or otherwise interact with the products and services of the data exporter (including Facebook and Instagram); information related to the things users do and the information users provide when using the services (such as profile information, posted photos and videos, shared location information, communications between users, and related information about use of the products and services); information related to the data subjects that other users of the products and services provide (such as a user's imported contacts or photos); information

related to users' networks and connections (such as a user's connections to groups, pages, and other users); information related to payments (such as information related to purchases or financial transactions); information about devices (such as information from or about the computers, phones or other devices where users install software provided by, or that access products and services of, the data exporter); information from websites and apps that use products and services of the data exporter (such as information about visits to third-party websites or apps that use a "like" or "comment" button or other service integrations); and information from third-party partners (such as information related to jointly offered services or use of third party services); and information from affiliates of Facebook and companies in the Facebook family of companies'.

130. As raised by some of the objections, it is therefore clear that the FB International Transfers found to be violating the GDPR concerns personal data including 'photographs, videos or messages' and 'everyday data of social interactions with family, friends, acquaintances and others'. Of particular relevance is the DE SAs view that 'a map of social contacts is very interesting for foreign law enforcement and intelligence', and that the transferred data allows 'not only to infer many matters of private and professional lives, but also allows to infer further data, including emotional and mental states' and 'can also be misused for political manipulation'.

131. In the same document it is also specified that special categories of data in the meaning of Article 9 GDPR are transferred. It is therefore clear that the FB International Transfers found to be violating the GDPR concern personal data including special categories of personal data, as also noted by the objections.

132. Meta IE argues that 'a large number of categories of data being involved' in the transfers does 'not equate to a large number of categories of personal data being "affected" by the (alleged infringement)'. However, for the reasons already explained in paragraphs 94 to 96 of this Binding Decision, the EDPB cannot accept this argument.

133. In light of the above assessment, the EDPB considers that a large number of categories of personal data have been affected by the infringement, including special categories of personal data under Article 9 GDPR. Therefore, this factor has to be taken into account when deciding on whether a fine should be imposed.

On the manner in which the infringement became known to the supervisory authorities (Article 83(2)(h) GDPR)

134. The DE SAs consider relevant that 'the infringement became known to the supervisory authority by a submission of a data subject, not by chance or report by the controller itself'. In this regard, Meta IE SA responds that 'The proposed finding of infringement arises from this own-volition inquiry. As noted above, however, Meta Ireland does not consider that there has been (or is) any infringement, and so never notified the alleged infringement to the DPC'.

135. The EDPB notes that the Inquiry is an own-volition inquiry, and not a complaint-based one. In any case, the EDPB considers that, as a rule, the circumstance that the infringement became known to the supervisory authority by a complaint or an investigation should be considered as neutral. The objections do not put forward reasons that would justify a departure from this rule in the present case.

136. Therefore, the EDPB is of the view that nothing arises to be taken into account here when deciding whether an administrative fine should be imposed on Meta IE.

On 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 (Article 83(2)(k) GDPR)

137. As the EDPB has previously explained, Article 83(2)(k) GDPR gives the supervisory authority room to take into account any other aggravating or mitigating factors applicable to the circumstances of the case in order to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case. For example, financial benefits gained, or losses avoided, directly or indirectly, from the infringement should be taken into account when deciding whether an administrative fine should be imposed. In addition, the EDPB recalls that the scope of Article 83(2)(k) GDPR is necessarily open-ended and should include all the reasoned considerations regarding the socio-economic context in which the controller or processor operates, those relating to the legal context and those concerning the market context. More specifically, economic gain from the infringement could be an aggravating circumstance if the case provides information about profit obtained as a result of the infringement of the GDPR.

138. The DE SAs provide an overview of the Meta Group's financial position - of which Meta IE is a part - in order to illustrate Meta IE's high profitability. In the DE SAs' view, Meta IE's turnover would not be possible without the data transfers to the US 'as it is a result of processing the data cumulatively by one infrastructure from different markets with all effectivity and efficiency that results from that'. However, according to the DE SAs, Meta IE has not made an effort to 'reinvest this turnover in order to withdraw the data from the US' and to 'build up data centres in the EU' which, in their view, allowed Meta IE to directly benefit from its own non-compliance and non-action to establish compliance. The DE SAs argue that 'the considerable economic and financial capacity should be taken into account when calculating the fine [...] even if there would be no specific financial benefit gained with the infringement or where it could not be determined and/or calculated'.

139. Meta IE responds to this by arguing that it has 'invested significantly in data centres' and already operated ones in the EU to support the provision of the Facebook service, but 'cannot "localise" the Facebook Service to support Meta Ireland Users solely from servers in the EU'. In addition, as noted by the IE SA in the Draft Decision, Meta IE's position is that, if it cannot make the FB International Transfers, it would not be in a position to provide its services in the EU/EEA. Meta IE explains that this is due to 'the inherently global, interconnected nature of the Facebook Service and the highly complex technical infrastructure that has been developed to support it'.

140. Given that Meta IE acknowledges that it would not be able to offer its services in the EU/EEA without performing the transfers, it can be inferred that transferring the data to the US in a way that infringes the GDPR is inextricably linked to the provision of the service to EU/EEA individuals. In this regard, the EDPB recalls that it is the business model which must adapt itself and comply with the requirements that the GDPR sets out in general and for each of the legal bases and not the reverse. Moreover, Meta IE indicates that the suspension order proposed by the IE SA would have 'severe consequences' for Meta IE and 'would clearly have a devastating impact on FIL's business, revenue and employees', which also suggests that a considerable part of its profits derived from the provision of the service in the EU arise from the breach of the GDPR.

*****

141. In summary, with respect to the assessment of the factors under Article 83(2) GDPR, the EDPB takes the view that, taking into account the scope of the processing, as well as the

very high number of data subjects affected, Meta IE committed an infringement of significant nature, gravity and duration. The EDPB also recalls its view that Meta IE committed the infringement at least with the highest degree of negligence, that a wide range of categories of personal data have been affected by the infringement, including special categories of personal data under Article 9 GDPR, and that the provision of the service by Meta IE in the EU is inextricably linked to the breach of the GDPR.

142. The analysis of the relevant factors under Article 83(2) GDPR speaks in favour of the need to impose an administrative fine. Now the EDPB proceeds with an assessment of the criteria under Article 83(1) GDPR.

*****

<u>The application of the criteria under Article 83(1) GDPR, in particular effectiveness and dissuasiveness</u>

143. The EDPB recalls that the administrative fine to be imposed in addition to the suspension order needs to be 'effective, proportionate and dissuasive' in accordance with Article 83(1) GDPR, which, read in conjunction with Recital 148 GDPR, makes it clear that the imposition of effective, proportionate and dissuasive fines, is a means to achieve the more general objective of effective enforcement of the GDPR.

144. As previously mentioned, the IE SA in its Draft Decision takes the view that the imposition of an administrative fine in addition to a suspension order 'would not be "effective, proportionate and dissuasive"' as required by Article 83(1) GDPR and 'would not render the DPC's response to the findings of unlawfulness any more effective'. In its Composite Response, the IE SA also notes that the objections and comments received by the CSAs 'broadly focus on concerns of deterrence and effectiveness'.

145. In Meta IE's view, 'the imposition of an administrative fine 'would not be "appropriate, necessary and proportionate", as required by Recital 129 GDPR' and as explained in the IE SA's Draft Decision.

146. The DE SAs, FR SA, ES SA and AT SA all raise concerns with regard to the effectiveness and dissuasiveness of the measures proposed by the Draft Decision and consider that the

imposition of a fine is necessary in order to meet the requirements of effectiveness and dissuasiveness under Article 83(1) GDPR.

147. As explained in the EDPB Guidelines on calculation of fines, a fine can be considered effective if it achieves the objectives with which it was imposed. The same reasoning applies to the choice of corrective measures under the GDPR in general. The EDPB recalls that the objective pursued by the corrective measure chosen can be to re-establish compliance with the rules, or to punish unlawful behaviour, or both. In addition, in accordance with Recital 148 GDPR, penalties including administrative fines should also be imposed 'in order to strengthen the enforcement of the rules of this Regulation'. As to dissuasiveness, the EDPB consistently recalls that a dissuasive fine is one that has a genuine deterrent effect.

148. The EDPB agrees with the ES and FR SAs' view that the suspension order proposed by the IE SA has a forward-looking nature, while an administrative fine would have a punitive effect with regard to the already committed or ongoing infringements. This position is reinforced by the AT SA's view that an administrative fine would be effective in the present case 'for counteracting the established infringement in the past'. Considering the wording of Article 58(2)(i) GDPR 'in addition to' and of Recital 148 GDPR 'penalties including administrative fines', the EDPB agrees with the ES, FR and AT SAs that the suspension order and an administrative fine would be compatible and complementary corrective measures.

149. The EDPB recalls that a fine is dissuasive where it prevents its addresses from infringing the objectives pursued and rules laid down by Union law. What is decisive in this regard is not only the nature and level of the fine but also the likelihood of it being imposed - anyone who commits an infringement must fear that the fine will in fact be imposed on them. In this regard, the criterion of dissuasiveness and that of effectiveness overlap, as they seek to produce similar effects. This has also been confirmed by AG Geelhoed who has explained that enforcement activities are considered 'effective' if they create a credible probability that, in case of non-compliance, the individuals or entities concerned run a high risk of being detected but also of being imposed sanctions which would at least deprive them of any economic benefit accruing from the transgression of the legal provisions at stake.

150. In that respect, the EDPB recalls that a distinction can be made between general deterrence (i.e. discouraging others from committing the same infringement in the future) and specific deterrence (i.e. discouraging the addressee of the fine from committing the same infringement again). The EDPB has previously held that, in order to ensure deterrence,

the fine must be set at a level that discourages both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the same or a similar unlawful conduct. The EDPB notes that all of the relevant and reasoned objections raise concerns with regard to the lack of general and specific deterrence of the proposed corrective measures.

151. As regards specific deterrence, the EDPB notes that according to the AT SA, 'Meta Ireland does not seem to have shown any efforts to refrain from transferring personal data to Meta Platforms, Inc.' but seems instead to have 'expressed that these data transfers are a fundamental requirement to be able to continue to provide its services in the EU/EEA area'. The AT SA derives from this that Meta IE 'might not be prepared to stop the data transfer in question'. In the same vein, the DE SAs consider that 'the individual case at hand does not allow to conclude that Meta is sufficiently deterred' because it has not recognised its non-compliance in the past and has not shown any form of active repentance. The DE SAs are concerned that a suspension order alone would not suffice to change the overall attitude of Meta towards general data protection compliance.

152. The EDPB shares the AT SA's and DE SAs' concerns. Indeed, there is nothing in the case file that allows the EDPB to consider that the imposition of a suspension order would be sufficient to achieve the effective and dissuasive effect that a fine can produce, as required under Article 83(1) GDPR. The EDPB recalls that Meta IE argues, throughout its submissions, that the applicable US law and practices relevant to the FB International Transfers, in conjunction with the appropriate safeguards provided pursuant to the 2021 SCCs, provide the requisite protection for Meta IE users' data for the purposes of Article 46(1) GDPR and therefore disagrees with the IE SA's finding of an infringement. The EDPB also takes note of Meta IE's criticism of the EDPB Recommendations on Supplementary Measures and of its view that they 'make a number of recommendations which appear to be based either on an erroneous interpretation of the CJEU Judgment and/or which seek to impose a higher standard upon data exporters seeking to rely on SCCs than the CJEU Judgment itself requires'. Moreover, Meta IE itself recognises that 'despite the TIA [Transfer Impact Assessment] being an assessment envisaged by the CJEU Judgment, the DPC did not request FIL's assessment prior to the issue of the PDD', so Meta IE did not present it proactively but only after the IE SA requested it.

153. The EDPB concurs with the FR SA's observation that suspending the unlawful transfer and bringing the processing into compliance with the GDPR is already an obligation resulting expressly from the GDPR and the Schrems II Judgment. The EDPB also agrees that the burden imposed by the suspension order is not greater than the burden which derives from the controller's legal obligations and that in the absence of a dissuasive effect arising from the final decision to be adopted by the IE SA, the controller will have no incentive to refrain from repeating its unlawful behaviour. As correctly noted by the FR SA, in the current version of the Draft Decision, 'the only risk for a controller who fails to comply with its obligation to suspend an unlawful transfer would be that a supervisory authority would order it to do so'.

154. In light of the above, the EDPB considers that on the basis of Meta IE's statements and position described in the above paragraphs, a suspension order alone would not be enough to produce the specific deterrence effect necessary to discourage Meta IE from continuing or committing again the same infringement.

155. As regards general deterrence, the EDPB agrees with the FR, DE and AT SAs' view that it is necessary to take into account not only the effect of the corrective measures in this particular case with regard to Meta IE, but also with regard to other controllers in general. More specifically, the AT SA points out that transferring data to the US is 'a widely used practice among numerous controllers' and that not imposing a fine on Meta IE would send a message that past infringements of the GDPR would not be properly addressed, which would also give no incentive to other controllers to comply with the GDPR. The FR SA highlights that, if an administrative fine is not imposed, other controllers transferring personal data under similar conditions as Meta IE would have no incentive to bring their transfers into conformity with the GDPR. Indeed, as the AT SA notes, the imposition of an administrative fine also has an awareness-raising function among other controllers who should be given a clear signal that non-compliance with the GDPR has consequences which also cover past behaviour.

156. The EDPB concurs with the AT SA view that if Meta IE is not fined for the infringement of Article 46(1) GDPR in the present case, other controllers might conclude that 'the cost of continuing an unlawful practice will outweigh the expected consequences of an infringement and will be less inclined to comply with the GDPR'. In the same vein, the DE SAs consider that if the only thing that the undertakings affected by the Schrems II Judgment

need to fear is an order to stop future transfers, then 'many managers might decide to just continue the transfer until they get caught'. In this regard, the EDPB recalls AG Geelhoed's explanation that the threat of repressive action must generate sufficient pressure to make non-compliance economically unattractive and therefore to ensure that compliance with the legal rules is realised in practice. In this regard, the EDPB takes note of the DE SAs observation that a fine would produce a deterrent effect if the costs of non-compliance with the GDPR are higher than the costs for compliance with the GDPR.

157. The EDPB agrees that the above-mentioned arguments are especially relevant in view of the high degree of responsibility of Meta IE as a controller. The DE SAs pointed out that Meta IE is an 'extremely profitable', 'data driven undertaking', whose turnover is 'almost completely a direct result of Meta IE's data processing'. Therefore, it is likely that Meta IE's behaviour has an impact on the behaviour of other controllers who would be inclined to follow the same model. The same is valid for the response of the supervisory authorities in case of an infringement - as pointed out by the DE SAs, if no fine is imposed on Meta IE by the IE SA, other controllers 'may demand to be treated by other supervisory authorities as the DPC treated Meta'.

158. In light of the above, the EDPB takes the view that the imposition of an administrative fine in addition to the suspension order would have an important deterrence effect, which the imposition of a suspension order alone cannot have. The additional imposition of an administrative fine in the present case would be effective and dissuasive especially because of the punitive element concerning the infringement that has already materialised, which the suspension order proposed by the IE SA lacks.

<u>The application of the criteria under Article 83(1) GDPR, in particular proportionality</u>

159. The EDPB recalls that the principle of proportionality is a general principle of EU law which has been explained by the CJEU on numerous occasions. It is consistent case-law that for a measure to be proportionate, it has to pursue a legitimate objective, be appropriate for attaining this legitimate objective, and not go beyond what is necessary to achieve it. More specifically, by virtue of that principle, measures imposing financial charges on economic operators are lawful provided that the measures are appropriate and necessary for meeting the objectives legitimately pursued. In addition, where there is a choice between

several appropriate measures, the least onerous measures must be used and the charges imposed must not be disproportionate to the aims pursued.

160. Therefore, the EDPB underlines that applying the principle of proportionality in the context of the present case requires a clear determination of the legitimate objective pursued by the imposition of an administrative fine in addition to the suspension order. Then, it is also necessary to ascertain that the imposition of an administrative fine in addition to the suspension order would be appropriate to attain the legitimate objective pursued and would not go beyond what is necessary in order to attain that objective. In order to assess this, due regard should be given to the circumstances of the case, as well as to the infringement viewed as a whole, account being taken, in particular, of the gravity of the infringement. More specifically, the imposition of an administrative fine should be proportionate both to the severity of the infringement and to the size of the undertaking to which the entity that committed the infringement belongs.

161. In this regard, the EDPB agrees with the DE SAs and AT SA view that the legitimate aim (or objective) pursued by the imposition of an administrative fine in the present case is to punish unlawful behaviour in order to ensure effective enforcement of and compliance with the GDPR and hence - protect the fundamental rights and freedoms of the data subjects.

162. As to the appropriateness (or suitability) of the measure to achieve the legitimate aim, the EDPB notes that according to Meta IE, the imposition of a fine would not be appropriate due to the complexities of this particular inquiry. Meta IE refers to the IE SA's statements in the Composite Response, and argues that 'the imposition of an administrative fine, by way of a punitive sanction, would be anything other than a disproportionate response in the circumstances of this particular case', especially where 'the objective of an administrative fine is to sanction wrongdoing that has already occurred'.

163. The EDPB is not swayed by Meta IE's reasoning. First, nothing in the Court's comments in paragraph 202 of the Schrems II judgment suggests that the imposition of an administrative fine in the present case would be inappropriate: the CJEU explains that in view of Article 49 GDPR, the annulment of an adequacy decision is not liable to create a legal vacuum, because it details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) GDPR or appropriate safeguards under Article 46 GDPR. Moreover, the IE SA examines in detail the possibility for Meta IE to rely on Article 49 GDPR for the transfers and concludes

that it is not open to Meta IE to rely on the derogations at Article 49(1) GDPR (or any of them).

164. Second, as explained above, the additional imposition of an administrative fine in the present case would be effective and dissuasive precisely because of the punitive element, which the suspension order proposed by the IE SA lacks. In this regard, the DE SAs rightly highlight that the 'effective enforcement can only be reached if the fine is effective and both special preventive and general preventive'. In the same vein, the AT SA considers that 'to strengthen enforcement of the GDPR, an administrative fine is effective in the present case for counteracting the established infringement in the past'.

165. Therefore, the EDPB takes the view that, in the circumstances of the present case as described above, the suspension order alone cannot achieve the objective pursued, namely to punish unlawful behaviour in order to ensure effective enforcement of the GDPR. Therefore, the IE SA is not in a situation where it has 'a choice between several appropriate measures' putting it under an obligation to choose the least onerous one because the suspension order and the fine pursue different objectives.

166. It is then necessary to assess whether the imposition of an administrative fine in addition to the suspension order would go beyond what is necessary to achieve the objective of ensuring effective enforcement of a GDPR through effective and dissuasive corrective measures.

167. The EDPB has already clarified that, in order to be effective, proportionate and dissuasive, a corrective measure should reflect the circumstances of the individual case, which include not only the specific elements of the infringement but also the specificities of the controller or processor's position, namely their financial position, as correctly observed by the AT SA. For example, the EDPB has previously recognised, in the context of the assessment of the proportionality of the fine under Article 83(1) GDPR, that an LSA can, in principle, consider a reduction on the grounds of the inability to pay the fine, if the requesting undertaking can demonstrate that its economic viability is jeopardised by the proposed fine. In addition, the EDPB has recognised that the difficult economic context in which a company is operating can be a factor to take into account, but has also recalled that the mere finding that an undertaking is in an adverse or loss-making financial situation does not automatically warrant a reduction of the amount of the fine.

168. Regarding Meta IE's size and financial capacity, the EDPB recalls the DE SAs' observations on the size and turnover of the Meta group, indicating that Meta IE is, indeed, a highly profitable undertaking and the imposition of a fine would not, in itself, be a disproportionate measure. The EDPB observes that Meta IE does not invoke concrete arguments to demonstrate that the imposition of an administrative fine would be disproportionate but merely refers to the IE SA statements in the Composite Response. The EDPB agrees with the ES SA's view that in terms of proportionality, Meta IE is 'an entity that generates huge profits, so imposing a fine taking into account the gravity of the infringement and the nature of the processing would not be disproportionate and would not cause it harm which it would not have to face as a result of acts contrary to the GDPR'. The EDPB also agrees with the AT SA's and DE SAs' view that, considering the assessment of the relevant factors referred to in Article 83(2) GDPR, the imposition of a fine would not be disproportionate.

<u>Conclusion</u>

169. In light of the above, the EDPB concludes that, considering the assessment carried out in this Binding Decision of the relevant factors under Article 83(2) GDPR referred to in the relevant and reasoned objections, namely the factors under Article 83(2)(a), (b), (d), (g), and (k) GDPR, as well as of the criteria under Article 83(1) GDPR, the IE SA's decision not to impose a fine for the breach by Meta IE of Article 46(1) GDPR does not comply with the GDPR. The EDPB considers that the imposition of a suspension order alone would not be sufficient to achieve the objective of effective enforcement of the GDPR.

170. Therefore, the EDPB takes the view that an administrative fine must be imposed on Meta IE for the breach of Article 46(1) GDPR.

171. In addition, the EDPB recalls that the factors under Article 83(2) GDPR also need to be given due regard by the IE SA in the calculation of the amount of the administrative fine, as the 'conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine'.

172. The EDPB Guidelines on the calculation of administrative fines indicate that when classifying the seriousness of the infringement and identifying the appropriate starting amount of the fine, in light of the circumstances of the specific case, the SA must give due regard to 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 (Article 83(2)(a) GDPR); the intentional or negligent character of the infringement (Article 83(2)(b) GDPR); and the categories of personal data affected by the infringement (Article 83(2)(g) GDPR).

173. In this regard, the EDPB recalls the gravity of the infringement at stake carried out by Meta IE, taking into account the particularly large scope of the processing and the very high number of data subjects affected, as well as the long duration of the infringement, which is still ongoing. The EDPB also reiterates its view that Meta IE committed the infringement of Article 46(1) with at least the highest degree of negligence. In addition, the EDPB recalls that a wide range of categories of personal data are affected by the infringement, including personal data covered by Article 9 GDPR. Therefore, based on the evaluation of the factors under Article 83(2)(a), (b) and (g) GDPR, the EDPB takes the view that the infringement is of a high level of seriousness.

174. The EDPB recalls that the Guidelines on calculation of fines indicate starting amounts for further calculation of the fine on the basis of whether the infringement is classified as being of a low, medium or high degree of seriousness. In accordance with the Guidelines on calculation of fines, the EDPB takes the view that the LSA should determine the starting amount for further calculation of the fine at a point between 20 and 100% of the applicable legal maximum. The EDPB recalls that starting amounts as expressed in the EDPB Guidelines on calculation of fines are starting points for further calculation while SAs have the discretion to utilise the full fining range ensuring that the fine is tailored to the circumstances of the case.

175. The EDPB also recalls that after having evaluated the nature, gravity and duration of the infringement as well as the intentional or negligent character of the infringement and the categories of personal data affected, account must also be taken of the remaining aggravating and mitigating factors under Article 83(2) GDPR.

176. In this respect, the EDPB reiterates its view that Meta IE bears a high degree of responsibility and that Meta IE's design of the FB service prevents it from providing this service in the EU/EEA without the FB International Transfers, which were found to be in breach of the GDPR. Consequently, the EDPB considers that the factors referred to in Article

83(2) (d) and (k) GDPR are aggravating and should be attributed sufficiently heavy weight in the calculation of the administrative fine by the LSA.

177. When calculating the final amount of the fine, the LSA should use the total worldwide annual turnover of the undertaking concerned for the preceding financial year, i.e. the worldwide annual turnover of all the entities composing the single undertaking. In the present case, this is the consolidated turnover of the group of companies headed by Meta Platforms, Inc. On the notion of 'preceding financial year', the event from which the preceding financial year should be considered is the date of the final decision taken by the LSA pursuant to Article 65(6) GDPR.

178. In light of the above, the EDPB instructs the IE SA to impose an administrative fine on Meta IE for the infringement of Article 46(1) GDPR that is in line with the principles of effectiveness, proportionality and dissuasiveness under Article 83(1), giving due regard to the relevant aggravating factors under Article 83(2) GDPR, namely the factors referred to in Article 83(2)(a), (b), (g), (d), (k) GDPR. When calculating the fine, the IE SA should take into consideration the total turnover of the group of companies headed by Meta Platforms, Inc. for the financial year preceding the adoption of the IE SA's final decision. The IE SA's assessment should be guided by the EDPB Guidelines on calculation of fines and the EDPB's assessment in this Binding Decision.

<u>Additional considerations</u>

179. For the sake of completeness, the EDPB also addresses Meta IE's allegations in its Article 65 Submissions that the imposition of an administrative fine would breach the general principle of equal treatment or non-discrimination and the principle of legal certainty.

180. As previously noted, Meta IE agrees with the IE SA's reasoning behind the decision not to impose an administrative fine for the breach of Article 46 GDPR set out in paragraphs 9.47 and 9.48 of the Draft Decision and considers this reasoning to be in line with Recital 129 and Article 58(2)(i) GDPR. The IE SA considers that the imposition of an administrative fine in this particular case would risk discriminating against Meta IE, given the absence of any corresponding fine in the decisions issued in response to the '101 complaints' regarding the use of Google Analytics introduced by NOYB following the Schrems II judgement, and given the absence of a comparable action taken vis-a-vis Google LLC. The EDPB also takes

note of Meta IE's argument that the imposition of an administrative fine 'would breach the principles of non-discrimination and equal treatment, which are fundamental principles of EU law' and 'would result in an entirely inconsistent application of the GDPR by the CSAs'. Meta IE also refers to the national decisions taken in response to the '101 complaints' regarding the use of Google Analytics, as well as to the 'EDPS CJEU Decision' and the 'EDPS EP Decision', and highlights that although infringements have been found in these decisions, no administrative fines have been imposed on the controllers concerned. In addition, Meta IE claims that the imposition of an administrative fine in the present case would be discriminatory against it and would violate the 'general principle of self-binding effect of the general practice followed by the supervisory authorities to date'. In addition, according to Meta IE, the imposition of an administrative fine on Meta Ireland would violate the principles of proportionality and legal certainty.

181. As regards the principles of equal treatment, the EDPB observes that the only argument Meta IE provides to substantiate its view that the imposition of an administrative fine would be discriminatory against it consists of a claim that the decisions adopted following the 101 complaints filled by NOYB and the observation that the EDPS decisions referred to have not imposed administrative fines on the controllers concerned in these cases. However, the EDPB considers that this allegation does not undermine the conclusion that the imposition of a fine was necessary in this particular case.

182. The principles of equal treatment, or non-discrimination, referred to by Meta IE is a general principle of European law that has been explained by the CJEU in the following terms: 'The different treatment of non-comparable situations does not lead automatically to the conclusion that there is discrimination. An appearance of discrimination in form may therefore correspond in fact to an absence of discrimination in substance. Discrimination in substance would consist in treating either similar situations differently or different situations identically'.

183. Therefore, the EDPB does not consider that the imposition of a fine in the present case would be discriminatory vis-a-vis Meta IE, merely because other controllers have not been fined in other cases where transfers have been deemed to be in breach of the GDPR following the Schrems II judgment. As Meta IE points out itself, Article 58(2)(i) GDPR grants each supervisory authority the power to 'impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the

circumstances of each individual case'. In addition, the EDPB recalls the CJEU's finding that 'when carrying out their duties, the supervisory authorities must act objectively and impartially'. A reference to 'individual cases' is also present in Article 65 GDPR, requiring the EDPB to ensure the consistent application of the GDPR in individual cases.

184. The CJEU has also recognised that discrimination 'cannot occur if inequality in the treatment of undertakings corresponds to an inequality in the situations of such undertakings'. In this regard, the EDPB notes that the similar or identical nature of the cases brought before the SAs and the EDPB has not been demonstrated by Meta IE. The EDPB also recalls that Articles 83(1) and (2) GDPR have been drafted in such a way as to prevent arbitrary and discriminatory decisions by the supervisory authorities - they provide clear rules and criteria to be taken into account by all SAs when enforcing the GDPR and when deciding on the most appropriate course of action depending on the seriousness of the infringements at stake. In this context, the EDPB has specified, with regard to Article 83(2)(k) GDPR, that it is 'fundamental importance for adjusting the amount of the fine to the specific case' and that 'it should be interpreted as an instance of the principle of fairness and justice applied to the individual case'.

185. The EDPB recalls that, pursuant to Article 70(1)(u) GDPR, one of its tasks is to ensure the consistent application of the GDPR by, among others, promoting the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities. Indeed, the need to ensure consistent application of the GDPR is particularly important in circumstances where the supervisory authorities handle complaints with identical content and which concern the same infringements committed by different controllers, as in the case of the '101 complaints'.

186. However, the dispute that the EDPB is called to resolve with this Binding Decision concerns a separate own-volition inquiry, the outcome of which is currently disputed before the EDPB by four CSAs. Therefore, the EDPB is under the legal obligation to take a decision on the merits of the objections in this individual case, in accordance with Recital 136 GDPR, Article 65(1)(a) GDPR and the EDPB Guidelines on Article 65(1)(a) GDPR. As the similarity of the cases referred to be Meta IE and the present case has not been demonstrated, the mere fact that in other cases no administrative fine has been imposed for the same infringement does not constitute discriminatory treatment against Meta IE.

187. the EDPB cannot accept Meta IE's argument that, by instructing the IE SA to impose on Meta IE an administrative fine for the breach of Article 46(1) GDPR would violate the principle of equal treatment or non-discrimination.

188. Furthermore, the EDPB cannot agree with Meta IE's view that the imposition of an administrative fine would breach the principle of legal certainty. The principle of legal certainty, also a general principle of EU law, requires that 'legal rules be clear and precise and aims to ensure that situations and legal relationships governed by EU law remain foreseeable'. This being said, the EDPB has previously recalled that it is settled case law that legal certainty is not absolute and undertakings are expected to take appropriate legal advice to anticipate the possible consequences of a rule and to assess the risk of infringement with 'special care'. In addition, the fact that the undertaking concerned has characterised wrongly in law its conduct upon which the finding of the infringement is based cannot have the effect of exempting it from imposition of a fine.

189. The EDPB considers that the GDPR lays down sufficiently clear and precise rules both with regard to the lawfulness of transfers of personal data to third countries and with regard to the exercise of corrective powers by the supervisory authorities in case of infringements, including the imposition of administrative fines. Also considering that Article 83(5)(c) GDPR subjects the infringements of Articles 44-49 GDPR to the highest administrative fine possible under the Regulation, the EDPB cannot agree that the imposition of a fine for the breach of Article 46(1) GDPR by Meta IE would be unforeseeable. In addition to the fact that the GDPR provides clear and precise rules on fines, the way in which the EDPB understands the correct application of Article 83 GDPR is explained in detail in the EDPB Guidelines on calculation of fines, which are public and easily accessible. Last but not least, the imposition and calculation of administrative fines is an issue that was addressed by the EDPB in all of its Binding Decisions to date, three of which relate to GDPR infringements committed by Meta IE.

190. In these circumstances, and taking into account the lack of further arguments put forward by Meta IE, the EDPB considers that the legal situation governed by the GDPR in the present case is sufficiently foreseeable and does not jeopardise the principle of legal certainty.

191. Therefore, EDPB considers that the application of the principles of equal treatment and legal certainty does not contradict the EDPB's conclusion that an administrative fine has to be imposed for the breach of Article 46(1) GDPR by Meta IE.

9.54 Article 83(2) GDPR provides that: *"(w)hen deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to [the criteria described in Article 83(2)(a) to (k)]*". In this regard, paragraph 88 of the Article 65 Decision records the EDPB's position that:

> *"88. Article 83(2) GDPR 'provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine': as explained in the EDPB Guidelines on Administrative Fines, this does not consist in 'a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case', and the 'conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice'."*

9.55 The EDPB reiterates the position at paragraph 171 of the Article 65 Decision:

> *"171. … the EDPB recalls that the factors under Article 83(2) GDPR also need to be given due regard by the IE SA in the calculation of the amount of the administrative fine, as the 'conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine'."*

9.56 It is therefore clear that, when calculating the amount of the administrative fine to be imposed, I must do so by reference to the assessments and determinations made by the EDPB for the purpose of Article 83 GPDR. Section 4.2.2 of the Article 65 Decision records the assessments, conclusions and determinations of the EDPB on the application of the Article 83(2) GDPR criteria to the particular circumstances of this case. Insofar as the Article 65 Decision records a clear and unequivocal determination of the EDPB concerning any aspect of the Article 83(2) GDPR assessment, the DPC cannot look behind that determination and is bound to apply it when calculating the quantum of the administrative fine to be imposed. This obligation arises as a result of the nature of the Article 65 Decision which, pursuant to Article 65(2) GDPR, is binding on the DPC and all CSAs. Where the Article 65 Decision does not record a clear and unequivocal determination of the EDPB on any aspect of the Article 83 GDPR assessment, the

DPC must exercise its own discretion. In any such case, the DPC must ensure to exercise its discretion in a manner that is consistent with the views that have been expressed by the EDPB in the Article 65 Decision. This obligation arises further to Article 65(6) GDPR, which requires the DPC to adopt its final decision "*on the basis of*" the EDPB's binding decision.

9.57 Against the background of the above, the following reflects the basis upon which the DPC will calculate the amount of the administrative fine to be imposed, by reference to the criteria set out in Article 83(2) GDPR, and the requirement, set out in Article 83(1) GDPR, for administrative fines to be "*effective, proportionate and dissuasive*" by reference to the circumstances of each individual case.

Meta Ireland's Final Submissions

9.58 By way of an annex to a letter dated 28 April 2023 ("the **Annex**"), the DPC invited Meta Ireland to exercise its right to be heard in response to the assessment set out below. Meta Ireland subsequently sought clarification, by way of letter dated 2 May 2023, in relation to the extent to which the DPC considered that it had the ability to exercise its own discretion on the matters identified in the Annex. The DPC confirmed, by way of letter dated 3 May 2023, that it only had the ability to exercise its own discretion insofar as the relevant aspect of the Article 83 GDPR assessment was not the subject of a clear and unequivocal determination of the EDPB. Meta Ireland furnished its final submissions, responding to the DPC's provisional Article 83 GDPR assessment on 8 May 2023 ("the **Final Submissions**").

9.59 The Final Submissions included a range of "preliminary objections"[211], under the following headings:

- "*Breach of the right to be heard*"
- "*Excess of competence by the EDPB*"
- "*Application of the Draft Fining Guidelines*"

9.60 The submissions made pursuant to these headings concern matters that have been determined by the EDPB itself, as part of the Article 65 process. As already outlined, the binding nature of an Article 65 decision and the clear and unequivocal nature of many of the determinations set out in the Article 65 Decision preclude the DPC from being able to take

[211] The Final Submissions, Section 2

account of these particular submissions in the context of this decision (i.e. the final decision of the DPC).

9.61 Otherwise, I have incorporated a summary of any submissions made by Meta Ireland within the relevant aspect of the Article 83 GDPR assessment, below.

The Article 83(2) Assessment: "the processing concerned"

9.62 For the purpose of the following assessment, "the processing concerned" should be understood as meaning the transfer of personal data under the controllership of Meta Ireland, from the EU/EEA to Meta Ireland's processor in the United States of America for the purposes of providing the Facebook service to its users. For ease of reference, the term "the Infringement" is used throughout the following assessment to denote the infringement of Article 46(1) GDPR.

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

Nature and Gravity of the Infringement

9.63 Paragraphs 90 and 91 of the Article 65 Decision record the EDPB's assessment that:

> *"90. With regard to the nature and gravity of the infringement, Meta IE argues that account has to be taken of the 'highly unusual circumstances of the alleged infringement of Article 46(1) GDPR' and in particular that 'Meta Ireland has always made the Meta Ireland Data Transfers in good faith'. The EDPB considers that this argument relates to Article 83(2)(b) GDPR rather than to Article 83(2)(a) GDPR and will examine it below.*
>
> *91. In its Draft Decision, when assessing the imposition of corrective measures for the established infringement of Article 46(1) GDPR, the IE SA underlines that 'the deficiencies in US law identified by the CJEU have not been addressed by the SCCs or supplemental measures, that a derogation under GDPR Article 49(1) is not available to Meta Ireland, and that the Data Transfers have been found to give rise to a breach of the essence of one or more fundamental rights'. In this regard, the EDPB highlights that an infringement giving rise to a breach of the essence of a fundamental right shall be considered as a grave one. In addition, the EDPB agrees with the arguments put*

forward by the AT SA, DE SAs, ES SA and FR SA, which consider that the infringement is particularly serious. More specifically, according to the ES SA, the FB International Transfers 'are not occasional or sporadic' but 'systematic, mass, repetitive and continuous in nature'. Likewise, the AT SA considers that Meta IE has been substantially and continuously violating data subject rights for several years. In the FR SA's view, the breach is particularly serious in terms of the data subjects' privacy. The DE SAs refer to the large number of data subjects concerned, the long period of the infringement and the scope of the processing."

Nature, Scope and Purpose of the Processing

9.64 Paragraph 92 of the Article 65 Decision records the EDPB's assessment that:

"92. Regarding the nature, scope and purpose of the processing concerned, the EDPB takes note of Meta IE's description of the processing as being 'simply the transfer of Meta Ireland User Data by Meta Ireland to its processor, MPI, in the US for the purpose of supporting Meta Ireland in its provision of the Facebook Service to Meta Ireland Users'. Specifically concerning the scope, Meta IE considers that the scale of the processing is not a relevant factor to assess whether to impose an administrative fine. Notwithstanding, the EDPB finds that Article 83(2)(a) GDPR entails that the scope or scale of the processing is a relevant factor when deciding whether to impose an administrative fine. More particularly, the EDPB recalls that the processing at stake has a particularly large scope and agrees with the DE SAs' view that the 'context of data processing extents to huge amounts of social interactions generated by these data subjects each and every day for the past and ongoing'. This is confirmed by the IE SA itself, which describes the transfers as 'systematic, bulk, repetitive and ongoing' throughout Section 8 of the Draft Decision."

Number of data subjects affected by the Infringement

9.65 Paragraphs 93 – 96 of the Article 65 Decision record the EDPB's assessment that:

"93. As to the number of data subjects affected, the EDPB considers the DE SAs' observation that Meta IE has '309 million daily active users in Europe' and that therefore 'a large share of the entire population of the European Union is directly affected by the non-compliance' of Meta IE' is particularly relevant. The same is supported by the FR and AT SAs, which also correctly observe that a 'particularly

massive volume of data' is at stake 'since the Facebook service has millions of users in the European Union' and that 'Meta is the provider of the biggest global social media network with an enormous number of users within the European Union and thus affected persons'.

94. Meta IE does not dispute the fact that 'a large number of data subjects have been involved' as the Facebook Service is used by a very high number of users. In its submissions on the Preliminary Draft Decision, Meta IE itself explains that 'Since its introduction in 2004, the Facebook Service has become an extremely popular and well-known online global communication and content sharing service, used by approximately 2.85 billion users globally every month to share and access information and connect with others around the world. This includes more than 255 million individual users in the EU / EEA'. However, according to Meta IE, 'the fact that personal data of a large number of data subjects have been involved in the Meta Ireland Data Transfers does not equate to a large number of data subjects being "affected" for the purpose of Article 83(1)(a) GDPR'. It further argues that 'There was always only an extremely limited practical risk of alleged interference with Meta Ireland Users' data protection and redress rights as a result of the Meta Ireland Data Transfer, and any such risk only involved an extremely limited number of Meta Ireland Users'.

95. The EDPB cannot agree with Meta IE's arguments. As explained in the EDPB Guidelines on calculation of fines, the number of data subjects affected should mean 'concretely but also potentially affected'. In other words, 'affected' data subjects are not only data subjects whose accounts have been subject to access requests, but also data subjects whose accounts could have been subject to access requests. The EDPB recalls that, at the time of this dispute resolution procedure, the infringement is still ongoing, which means that the personal data of Facebook users is transferred to and processed in the US without appropriate safeguards, as required by Article 46(1) GDPR.

96. Therefore, the EDPB concludes that a very high number of data subjects is affected and this already high number can keep increasing until the infringement is effectively brought to an end."

Duration of the Infringement

9.66 Paragraphs 97 – 99 of the Article 65 Decision records the EDPB's assessment that:

"97. Regarding the duration of the infringement, the DE SAs and AT SA stress that it has been ongoing for several years, which they see as an aggravating factor. According to the AT SA, the duration of the infringement resulted in data subjects' rights being 'substantially and continuously violated'. The DE SAs point out that 'the duration of the infringement for the data subjects extents to even before GDPR with the previous regimen with the same legal obligations for controllers'. The DE SAs further highlight that 'the data processing of the undertaking is under scrutiny of supervisory authorities since about ten years'. Meta IE responds to this by stressing that the inquiry only concerns the period since the GDPR became applicable.

98. The EDPB takes note of the IE SA's explanation that the purpose of the Draft Decision is 'to consider whether Meta Ireland is acting [...] compatibly with GDPR Article 46(1), in making transfers [...] of personal data relating [...] to Meta US pursuant to standard contractual clauses [...], following the judgment of the Court of Justice of the European Union ("the CJEU"), delivered on 16 July 2020, in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems'. The EDPB also notes that no CSA raised objections concerning the temporal scope of the Draft Decision. Therefore, the starting point of the infringement at stake should be determined on the basis of the description made in the Draft Decision only, i.e. from 16 July 2020 (date of the adoption of the Schrems II judgment). The EDPB considers that this duration of infringement is significant and has to be taken into account when deciding whether an administrative fine should be imposed."

9.67 At paragraph 99 of the Article 65 Decision, the EDPB records its conclusion as follows:

"As a conclusion, the EDPB considers that, taking into account the nature and scope of the processing, as well as the very high number of data subjects affected, Meta IE committed an infringement of significant nature, gravity and duration. Therefore, this criterion has to be taken into account when deciding whether an administrative fine should be imposed."

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

9.68 Paragraphs 103 – 115 of the Article 65 Decision record the EDPB's assessment of this aspect of matters:

"103. As already clarified in the EDPB Guidelines on Administrative Fines, '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'. In other words, the EDPB Guidelines on calculation of fines confirm that there are two cumulative elements on the basis of which an infringement can be considered intentional: the knowledge of the breach and the wilfulness in relation to such act. On the other hand, an infringement is 'unintentional' when there was a breach of the duty of care, without having intentionally caused the infringement. The EDPB also recalls that the intentional or negligent character of the infringement 'should be assessed taking into account the objective elements of conduct gathered from the facts of the case' and that 'depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence'.

104. The EDPB notes and agrees with the DE SAs' observation that Meta IE has been 'under scrutiny of supervisory authorities since about ten years': the two landmark judgments issued by the CJEU in 2015 and in 2020 were also issued in cases concerning this same company. Indeed, as recalled by the IE SA in the Draft Decision, the original complaint against Meta IE which contended that the transfer of personal data by Meta IE to Meta Platforms, Inc., in reliance on the 'Safe Harbor' adequacy decision, was unlawful and which led to judicial proceedings in Ireland and then to the preliminary ruling of the CJEU in 2015 in the case C-362/14, Schrems v Data Protection Commissioner ('Schrems I judgment'), was filed by Schrems with the IE SA on 25 June 2013. The Schrems II Judgment, as previously mentioned, was handed down by the CJEU on 16 July 2020. Following the IE SA Preliminary Draft Decision of 28 August 2020 and the opening of inquiry IN 20-8-1, Meta IE commenced judicial proceedings against the IE SA.

105. In addition, the EDPB takes note of Section 7 of the Draft Decision, where the IE SA first sets out the framework of its assessment and then examines in detail the lawfulness of the transfers, by following the terms of Article 46(1) GDPR as reflected by the Schrems II Judgment. The EDPB also takes note of the IE SA's assessment in Section 8 of the Draft Decision and the conclusion that it is 'not open to Meta Ireland to rely on the derogations at Article 49(1) (or any of them) to justify the systematic, bulk, repetitive and ongoing transfers of its users' data from the EU to the US'.

106. The EDPB recalls the IE SA's conclusion that the 2021 SCCs Meta IE relied upon to carry out the FB International Transfers could not remedy the inadequate protection afforded by US law. The EDPB also notes that the IE SA examined in detail the question of whether Meta IE has put in place supplementary measures that could address the insufficiencies of the protection provided by US Law and its conclusion that this is not the case.

107. As explained by the EDPB in its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (hereinafter 'EDPB Recommendations on Supplementary Measures'), when assessing third countries and identifying appropriate supplementary measures, controllers should assess if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools that they are relying on. In this regard, the EDPB notes that, according to Meta IE's assessment, 'the level of protection required by EU law is provided for by relevant US law and practice' and that Meta IE implemented supplementary measures in addition to the 2021 SCCS in order to 'further ensure that an adequate level of protection continues to apply to User Data transferred from FIL to FB, Inc'. In other words, Meta IE has implemented supplementary measures on the basis of an assessment which concluded that there was no need for such measures, since, in Meta IE's view, the relevant US law and practice were already providing a level of protection equivalent to the one provided under EU law.

108. Moreover, the EDPB highlights the IE SA's concern that Meta IE's submissions 'seem to simply ignore the ruling of the CJEU' and 'that Meta Ireland is seeking to promote a lower standard for the objective of SCCs and supplemental measures than is permitted by the Judgment and the GDPR'. More specifically, the IE SA notes that Meta IE 'seems to identify its own test for determining suitability of supplemental measures by lowering the standard to include measures that can "address" or "mitigate" any "relevant remaining" inadequacies in the protections offered by US law and practice and the SCCs', and concludes in the Draft Decision that 'Meta Ireland does not have in place any supplemental measures which would compensate for the inadequate protection provided by US law'.

109. Considering the detailed assessment of the US legal system by the CJEU in the Schrems II judgment, the series of steps to follow, sources of information and examples

of supplementary measures provided in the EDPB Recommendations on Supplementary Measures', as well as the IE SA's findings in the Preliminary Draft Decision and Revised Preliminary Draft Decision which were shared with Meta IE prior to the Draft Decision, the EDPB takes the view that Meta IE could not have been unaware of the fact that the FB International Transfers could be considered in violation of Article 46(1) GDPR.

110. In light of the above, the EDPB concludes that there are sufficient indications that Meta IE committed the infringement of Article 46(1) GDPR knowingly.

111. Additionally, with respect to the finding of the IE SA that reliance on Article 49 GDPR was not open to Meta IE for the purpose of carrying out the FB International Transfers, the EDPB is of the view that at the very least Meta IE could not have been unaware of the guidance of the EDPB and of the findings of the CJEU that the derogations cannot be relied upon for systematic and massive transfers and have to be strictly construed.

112. As regards the 'wilfulness' component of intent, the EDPB recalls that the CJEU has established a high threshold in order to consider an act intentional. The EDPB has previously recalled that even in criminal proceedings, the CJEU has acknowledged the existence of 'serious negligence', rather than 'intentionality' when 'the person responsible commits a patent breach of the duty of care which he should have and could have complied with in view of his attributes, knowledge, abilities and individual situation'. Although a company for which the processing of personal data is at the core of its business activities is expected to have sufficient measures in place for the safeguard of personal data and for the thorough understanding of its duties in this regard, this does not per se demonstrate the wilfulness of an infringement. In this regard, the EDPB notes that Meta IE has taken steps in order to achieve compliance with Chapter V of the GDPR following the Schrems II judgment, but these steps were not sufficient to achieve compliance as established by the Draft Decision. Consequently, the EDPB takes the view that, on the basis of the objective elements in the case file, 'wilfulness' on the side of Meta IE is not fully demonstrated.

113. Nevertheless, the EDPB stresses that Meta IE's position that the relevant US law and practice were already providing a level of protection equivalent to the one provided under EU law in spite of the Schrems II judgment, the lower standard applied

by Meta IE when implementing the SCCs and supplementary measures, as well as the subsequent failure to implement supplementary measures that were aimed to compensate (and could compensate) for the inadequate protection provided by US law (rather than address or mitigate 'any relevant remaining inadequacies in the protection afforded by US law and practice', as argued by Meta IE), indicate a very high degree of negligence on the side of Meta IE. As the IE SA correctly recalls, 'the terms "mitigate" and "address" cannot be found in either the Judgment or the GDPR'. In addition, the EDPB notes that Meta IE contests the IE SA's interpretation of the Schrems II judgment and of the test for determining suitability of supplementary measures not only in its submissions on the Preliminary Draft Decision, but also in its submissions on the Revised Preliminary Draft Decision. Therefore, it appears that, by not applying the correct test for determining the suitability of supplementary measures in spite of the clear requirement that the appropriate safeguards to be taken by the controller must 'compensate for' the lack of data protection in the third country, Meta IE breached its duty of care and acted at least with the highest degree of negligence.

114. This is the case also in light of the arguments brought by the AT SA and DE SAs 264 that Meta IE has acted at least with conditional intent (dolus eventualis) 'since it must have seriously considered a violation of Chapter V GDPR when carrying out data transfers'. The EDPB has previously explained that 'Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence'.

115. In light of the above, the EDPB takes the view that Meta IE committed the infringement at least with the highest degree of negligence and this has to be taken into account when deciding whether an administrative fine should be imposed."

Article 83(2)(c): any action taken by the controller to mitigate the damage suffered by data subjects

9.69 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. In the Annex, I noted that Meta Ireland, throughout the course of the inquiry, considered that the processing concerned was being carried out on a lawful basis. That being the case, I considered that it followed that Meta Ireland could not have been expected to take action "*to mitigate the damage suffered by data subjects*" in circumstances where it did not consider any infringement to have occurred or any damage to have been suffered by data subjects. In the

circumstances, I expressed the view, in the Annex, that nothing arises for consideration under this heading.

9.70 By way of the Final Submissions, Meta Ireland submitted[212] that:

> *"4.3 Meta Ireland respectfully submits that the DPC has erred in taking the view that, because Meta Ireland considers that (i) the Data Transfers have been made in compliance with Chapter V GDPR at all material times and (ii) no damage has been suffered by data subjects, nothing arises for consideration in respect of Articles 83(2)(c) and (f) GDPR.*
>
> *4.4 Specifically, the DPC has failed to have any or any adequate regard to the actions taken by Meta Ireland to mitigate any possible adverse effects or damage to data subjects and Meta Ireland's full cooperation with the DPC throughout the Inquiry. Relevant actions taken by Meta Ireland voluntarily to assist Meta Ireland users following Schrems II include the following:*
>
> > *(A) Providing users with a significant amount of additional information about the Data Transfers beyond that required by Article 13(1)(f) GDPR, the potential impact on them arising from such transfers, including the potential for access to personal data by the US Government, and the measures in place to protect users. This enabled EU/EEA users to make fully informed choices as to whether to continue to use Facebook, and ensured their transparency rights under the GDPR were fully respected;*
> >
> > *(B) Following the adoption of the 2021 SCCs, which were intended to address Schrems II, quickly taking all steps necessary to ensure the Data Transfers were made pursuant to the 2021 SCCs, thereby affording data subjects the additional safeguards and rights provided for therein; and*
> >
> > *(C) Implementing supplementary measures which provided additional safeguards in respect of the Data Transfers, each as described in greater detail in Meta Ireland's submissions in the Inquiry.*
>
> *4.5 Meta Ireland requests, therefore, that the DPC reconsiders its provisional decision that nothing arises for consideration in respect of the factors referred to at Articles*

[212] The Final Submissions, Section 4, paragraphs 4.3 to 4.5 (inclusive)

83(2)(c) and (f) GDPR, and instead treats the actions summarised above and Meta Ireland's cooperation with the DPC throughout the Inquiry as significantly mitigating."

9.71 In relation to the suggestion that the DPC failed to take account of "*Meta Ireland's full cooperation with the DPC throughout the inquiry*", I will address this submission as part of the Article 83(2)(f) assessment, below.

9.72 In terms of the identified actions that were voluntarily undertaken by Meta Ireland "*to assist Meta Ireland users following Schrems II*", my views are as follows: in relation to the provision, to Users, of "*a significant amount of additional information about the Data Transfers beyond that required by Article 13(1)(f) GDPR*" ("the **Additional Information**"), I note that the assessment required to be undertaken, pursuant to Article 83(2)(c) GDPR, is the assessment of "*any action taken by the controller … to mitigate the damage suffered by data subjects*".

9.73 The Article 65 Decision does not address the "*damage suffered by data subjects*" as a result of the Infringement. It does, however, detail the EDPB's views, as regards the risks to the fundamental rights and freedoms of data subjects arising from the Infringement. At paragraph 122 of the Article 65 Decision, the EDPB records its view that the Data Transfers result in "*a high residual risk for the rights and freedoms of the data subjects concerned, because, as highlighted [in the Draft Decision], data subjects are still not protected against 702 FISA DOWNSTREAM (PRISM) requests and Meta US would still be required to disclose its users' personal data, if requested by the US Government*". Considering the damage that might flow from this risk, if materialised, it seems clear that the resulting damage (where the risk to materialise) would comprise, at least, the loss of control over one's personal data.

9.74 While I acknowledge that the provision of the Additional Information to Users about the Data Transfers (including in relation to the potential for access to personal data by the US Government) would help them to make "*fully informed choices as to whether to continue to use Facebook*[213]", my view is that the impact of the Additional Information, in terms of its potential to mitigate the damage identified above, is limited in circumstances where it places the obligation on individual users to seek out and engage with the information and to decide whether they wish to accept the risk of access by the US Government associated with continued use of the Facebook service.

[213] The Final Submissions, Section 4, paragraph 4.4(A)

9.75 In the circumstances, I consider it appropriate for me to take account, as a mitigating factor for the purpose of the Article 83(2)(c) GDPR assessment, the fact that Meta Ireland provides the Additional Information to Users. In terms of the weight that I might attribute to this factor, however, its limited ability to mitigate the loss of control that would result from access, by the US Government, to Users' personal data means that the weight that I might attribute to this mitigating factor is also limited.

9.76 In relation to the other identified actions[214], namely "*quickly taking of all steps necessary to ensure the Data Transfers were made pursuant to the 2021 SCCs, thereby affording data subjects the additional safeguards and rights provided for therein*" and *"[i]mplementing supplementary measures which provided additional safeguards in respect of the Data Transfers*", I am unable to take these matters into account as mitigating factors in circumstances where this would be inconsistent with the views that have been expressed by the EDPB in the Article 65 Decision[215].

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

9.77 Paragraphs 116 to 125 of the Article 65 Decision records the EDPB's assessment of this aspect of matters:

> "*116. The EDPB recalls that, pursuant to Article 83(2)(d) GDPR, the degree of responsibility of the controller or processor will have to be assessed, taking into account measures implemented by them to meet the requirements of data protection by design and by default (Article 25 GDPR) and of security of processing (Article 32 GDPR). More specifically, the EDPB has explained that 'the question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation'. In addition, the residual risk for the freedoms and rights of the data subjects, the impairment caused to the data subjects and the damage persisting after the adoption of the measures by the controller as well as the degree of robustness of the measures adopted pursuant to Articles 25 and 32 GDPR must be assessed.*

[214] The Final Submissions, Section 4, paragraph 4.4(B) and (C)
[215] See, for example, paragraph 121 of the Article 65 Decision

117. The EDPB has also explained that, given the increased level of accountability under the GDPR, it is likely that this factor will be considered either an aggravating or a neutral one. Only in exceptional circumstances, where the controller or processor has gone above and beyond the obligations imposed upon them, will this be considered a mitigating factor.

118. Meta IE argues that 'the issue regarding EU-US data transfers is fundamentally one of a "conflict of laws" between the EU and the US' and that it has conducted all appropriate assessments, maintained all documentation and taken all steps available to it as soon as possible, such as entering into the 2021 SCCs.

119. The EDPB considers that these arguments have no bearing on the degree of responsibility of Meta IE in the present case.

120. It is clear from Article 25(1) GDPR that the controller is under an obligation, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. In addition, Article 32(1) GDPR lays down an obligation for the controller, by taking into account a number of factors, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons. Article 32(2) GDPR further specifies that, in assessing the level of security, account shall be taken in particular of the risks that are presented by processing, in particular from [...] unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

121. In this regard, the EDPB recalls that the IE SA carries out a detailed assessment of whether Meta IE implemented supplementary measures that could address the inadequate protection provided by US law. More specifically, the IE SA analyses the organisational, technical and legal measures implemented by Meta IE and concludes that these measures cannot, 'whether viewed in isolation, or in tandem with the 2021 SCCs and the full suite of measures outlined in the ROS', compensate for the deficiencies identified in US law and cannot provide essentially equivalent protection to that available under EU law.

122. This results in a high residual risk for the rights and freedoms of the data subjects concerned, because, as highlighted by the IE SA, data subjects are still not protected against 702 FISA DOWNSTREAM (PRISM) requests and Meta US would still be required to disclose its users' personal data, if requested by the US Government.

123. It is relevant also to recall that the EDPB Recommendations 1/2020 clarified that controllers may have to apply some or all of the measures described therein even irrespective of the level of protection provided for by the laws applicable to the data importer because they need to comply with Articles 25 and 32 GDPR in the concrete circumstances of the transfers.

124. Against this background, the EDPB recalls the DE SAs view that, considering the amount of data processed, 'the responsibility may have been heightened above average'. The EDPB also finds particularly relevant the FR SA's observation that the Facebook social network occupies an 'inescapable place in France' since it 'dominates by far the social media market' and, due to its dominant position, generates important 'network effects'. The EDPB considers that this is the case not only in France, but in the EEA in general. In addition, the Facebook service is provided to many users who do not necessarily have legal or technical knowledge. These users rely on the information published by Meta IE and therefore would reasonably expect that their personal data is protected when it is transferred to the US. Finally, the EDPB concurs with the FR SA's view that 'in parallel with its traditional function of maintaining and developing interpersonal relationships, this social network also occupies an increasingly larger role in areas as diverse as access to information, public debate or even civil security'.

125. In light of the above considerations, the EDPB takes the view that there are enough elements in the analysis of this factor which confirm Meta IE's high degree of responsibility. Therefore, this factor has be taken into account when deciding whether to impose an administrative fine."

Article 83(2)(e): any relevant previous infringements by the controller

9.78 Paragraphs 126 and 127 of the Article 65 Decision record the EPDB's assessment of this aspect of matters:

"126. The EDPB recalls that, according to Article 83(2)(e) GDPR and Recital 148 GDPR, any relevant previous infringements committed by the controller or processor are to

given due regard when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine. In addition, the absence of any previous infringements cannot be considered a mitigating factor, as compliance with the GDPR is the norm and if there are no previous infringements, this factor can be regarded as neutral. The EDPB has already explained that prior infringements are relevant as they might provide an indication about the controller's general attitude towards the observance of the GDPR and that recent infringements under the GDPR have more significance than infringements that have taken place long time ago.

127. In this regard, the EDPB notes the AT SA's remark that 'it is not the first case where the DPC has established a violation of the GDPR by Meta Ireland'. The AT SA Objection does not make reference to specific cases where the IE SA has established a violation of the GDPR by Meta IE, but it is possible to recall in particular the IE SA's decisions adopted following EDPB Binding Decisions 2/2022 of 28 July 2022 and 3/2022 and 4/2022 of 5 December 2022 where the IE SA found that Meta IE breached the GDPR. The EDPB recalls that at the time when the Draft Decision was circulated to the CSAs, the IE SA's final decision in these cases had not yet been adopted. Therefore, nothing arises to be taken into account here when deciding whether an administrative fine should be imposed on Meta IE."

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

9.79 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. In the circumstances, I proposed, in the Annex, to conclude that nothing arises for consideration under this heading.

9.80 By way of paragraph 4.4 of the Final Submissions, Meta Ireland submitted that I should take account of its full cooperation with the DPC throughout the Inquiry as a significantly mitigating factor. While acknowledging Meta Ireland's full cooperation during the course of the within Inquiry, I note that it is required to do so by Article 31 GDPR, which requires data controllers and processors to "*cooperate, on request, with the supervisory authority in the performance of its tasks*". I secondly note that the assessment required to be carried out, pursuant to Article 83(2)(f) GDPR, is "*the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement*" [emphasis added]. It is therefore clear that the cooperation that would be relevant for assessment, here,

is the cooperation that has taken place for the purpose of remedying the Infringement and mitigating the possible adverse effects on data subjects. I note, in this regard, that I have already taken account, within the Article 83(2)(c) assessment, above, of the actions taken by Meta Ireland in an effort to mitigate the possible adverse effects of the Infringement on data subjects. That being the case, it is not open to me to take those same matters into account for a second time within the same Article 83(2) assessment.

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

9.81 Paragraphs 128 to 133 of the Article 65 Decision record the EDPB's assessment of this aspect of matters:

> *"128. Concerning the requirement to take account of the categories of personal data affected under Article 83(2)(g) GDPR, the EDPB recalls that the GDPR clearly highlights the types of data that deserve special protection and therefore a stricter response in terms of fines. The EDPB has already explained that categories of personal data deserving a stricter response in terms of fines include at the very least, the types of data covered by Articles 9 and 10 GDPR, and data outside the scope of these Articles the dissemination of which causes immediate damages or distress to the data subject, such as location data, data on private communication, national identification numbers, or financial data.*
>
> *129. The EDPB takes note of the large number of categories of personal data transferred to the US, as outlined in the Draft Decision. More specifically, Part A of Appendix 1 to the Meta US's Data Transfer and Processing Agreement of 25 May 2018 mentions: 'the personal data generated, shared and uploaded by or about individuals who visit, access, use or otherwise interact with the products and services of the data exporter (including Facebook and Instagram); information related to the things users do and the information users provide when using the services (such as profile information, posted photos and videos, shared location information, communications between users, and related information about use of the products and services); information related to the data subjects that other users of the products and services provide (such as a user's imported contacts or photos); information related to users' networks and connections (such as a user's connections to groups, pages, and other users); information related to payments (such as information related to purchases or financial transactions); information about devices (such as information from or about*

the computers, phones or other devices where users install software provided by, or that access products and services of, the data exporter); information from websites and apps that use products and services of the data exporter (such as information about visits to third-party websites or apps that use a "like" or "comment" button or other service integrations); and information from third-party partners (such as information related to jointly offered services or use of third party services); and information from affiliates of Facebook and companies in the Facebook family of companies'.

130. As raised by some of the objections, it is therefore clear that the FB International Transfers found to be violating the GDPR concerns personal data including 'photographs, videos or messages' and 'everyday data of social interactions with family, friends, acquaintances and others'. Of particular relevance is the DE SAs view that 'a map of social contacts is very interesting for foreign law enforcement and intelligence', and that the transferred data allows 'not only to infer many matters of private and professional lives, but also allows to infer further data, including emotional and mental states' and 'can also be misused for political manipulation'.

131. In the same document it is also specified that special categories of data in the meaning of Article 9 GDPR are transferred. It is therefore clear that the FB International Transfers found to be violating the GDPR concern personal data including special categories of personal data, as also noted by the objections.

132. Meta IE argues that 'a large number of categories of data being involved' in the transfers does 'not equate to a large number of categories of personal data being "affected" by the (alleged infringement)'. However, for the reasons already explained in paragraphs 94 to 96 of this Binding Decision, the EDPB cannot accept this argument.

133. In light of the above assessment, the EDPB considers that a large number of categories of personal data have been affected by the infringement, including special categories of personal data under Article 9 GDPR. Therefore, this factor has to be taken into account when deciding on whether a fine should be imposed."

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

9.82 Paragraphs 134 – 136 of the Article 65 Decision record the EDPB's assessment of this aspect of matters:

> *"134. The DE SAs consider relevant that 'the infringement became known to the supervisory authority by a submission of a data subject, not by chance or report by the controller itself'. In this regard, Meta IE SA responds that 'The proposed finding of infringement arises from this own-volition inquiry. As noted above, however, Meta Ireland does not consider that there has been (or is) any infringement, and so never notified the alleged infringement to the DPC'.*
>
> *135. The EDPB notes that the Inquiry is an own-volition inquiry, and not a complaint-based one. In any case, the EDPB considers that, as a rule, the circumstance that the infringement became known to the supervisory authority by a complaint or an investigation should be considered as neutral. The objections do not put forward reasons that would justify a departure from this rule in the present case.*
>
> *136. Therefore, the EDPB is of the view that nothing arises to be taken into account here when deciding whether an administrative fine should be imposed on Meta IE."*

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

9.83 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The DPC notes that measures have not previously been ordered against Meta Ireland with regard to the same subject matter. In the circumstances, the DPC considers that nothing arises for consideration under this heading.

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

9.84 The EDPB (in the Article 65 Decision) has not addressed this aspect of matters. The DPC considers that nothing arises for assessment under this heading.

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

9.85 Paragraphs 137 to 140 of the Article 65 Decision record the EDPB's assessment of this aspect of matters:

"137. As the EDPB has previously explained, Article 83(2)(k) GDPR gives the supervisory authority room to take into account any other aggravating or mitigating factors applicable to the circumstances of the case in order to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case. For example, financial benefits gained, or losses avoided, directly or indirectly, from the infringement should be taken into account when deciding whether an administrative fine should be imposed. In addition, the EDPB recalls that the scope of Article 83(2)(k) GDPR is necessarily open-ended and should include all the reasoned considerations regarding the socio-economic context in which the controller or processor operates, those relating to the legal context and those concerning the market context. More specifically, economic gain from the infringement could be an aggravating circumstance if the case provides information about profit obtained as a result of the infringement of the GDPR.

138. The DE SAs provide an overview of the Meta Group's financial position - of which Meta IE is a part - in order to illustrate Meta IE's high profitability. In the DE SAs' view, Meta IE's turnover would not be possible without the data transfers to the US 'as it is a result of processing the data cumulatively by one infrastructure from different markets with all effectivity and efficiency that results from that'. However, according to the DE SAs, Meta IE has not made an effort to 'reinvest this turnover in order to withdraw the data from the US' and to 'build up data centres in the EU' which, in their view, allowed Meta IE to directly benefit from its own non-compliance and non-action to establish compliance. The DE SAs argue that 'the considerable economic and financial capacity should be taken into account when calculating the fine [...] even if there would be no specific financial benefit gained with the infringement or where it could not be determined and/or calculated'.

139. Meta IE responds to this by arguing that it has 'invested significantly in data centres' and already operated ones in the EU to support the provision of the Facebook service, but 'cannot "localise" the Facebook Service to support Meta Ireland Users solely from servers in the EU'. In addition, as noted by the IE SA in the Draft Decision, Meta IE's position is that, if it cannot make the FB International Transfers, it would not be in a position to provide its services in the EU/EEA. Meta IE explains that this is due to 'the inherently global, interconnected nature of the Facebook Service and the highly complex technical infrastructure that has been developed to support it'.

140. Given that Meta IE acknowledges that it would not be able to offer its services in the EU/EEA without performing the transfers, it can be inferred that transferring the data to the US in a way that infringes the GDPR is inextricably linked to the provision of the service to EU/EEA individuals. In this regard, the EDPB recalls that it is the business model which must adapt itself and comply with the requirements that the GDPR sets out in general and for each of the legal bases and not the reverse. Moreover, Meta IE indicates that the suspension order proposed by the IE SA would have 'severe consequences' for Meta IE and 'would clearly have a devastating impact on FIL's business, revenue and employees', which also suggests that a considerable part of its profits derived from the provision of the service in the EU arise from the breach of the GDPR."

Summary Conclusion of the EDPB

9.86 At paragraphs 141 and 142 of the Article 65 Decision, the EDPB records its conclusion that:

"141. In summary, with respect to the assessment of the factors under Article 83(2) GDPR, the EDPB takes the view that, taking into account the scope of the processing, as well as the very high number of data subjects affected, Meta IE committed an infringement of significant nature, gravity and duration. The EDPB also recalls its view that Meta IE committed the infringement at least with the highest degree of negligence, that a wide range of categories of personal data have been affected by the infringement, including special categories of personal data under Article 9 GDPR, and that the provision of the service by Meta IE in the EU is inextricably linked to the breach of the GDPR.

142. The analysis of the relevant factors under Article 83(2) GDPR speaks in favour of the need to impose an administrative fine. Now the EDPB proceeds with an assessment of the criteria under Article 83(1) GDPR."

9.87 The EDPB then proceeded to carry out an assessment of the criteria under Article 83(1) GDPR, namely the requirement for administrative fines, in each individual case, to be "*effective, proportionate and dissuasive*". That assessment is recorded at paragraphs 143 to 178 of the Article 65 Decision. It is important to note, in this regard, that that assessment concerned the EDPB's proposal to include, in its binding decision, a requirement for the DPC to impose an administrative fine on Meta Ireland. A separate assessment, for the purpose of Article 83(1) GDPR, must be carried out by the DPC by reference to the fine to be imposed by way of this

final decision. While the DPC will be required to exercise its own discretion, in this regard, the binding nature of the Article 65 Decision and the requirement, set out in Article 65(6) GDPR, for the DPC to adopt its final decision "*on the basis of*" the Article 65 Decision mean that the DPC must ensure to exercise its discretion in a manner that it not inconsistent with the views expressed, and determinations made, by the EDPB in the Article 65 Decision. That assessment is set out, further below.

Assessment of Quantum

9.88 As already noted, the EDPB assessments set out above reflect the EDPB's views on the application of the Article 83(2) GDPR criteria, as regards both the determination of whether or not an administrative fine ought to be imposed and the determination of the amount of any such fine.

9.89 As noted, above, nothing arises for consideration pursuant to Articles 83(2)(e), (f), (h), (i) and (j). I have recorded my view that Meta Ireland's provision of the Additional Information ought to be taken into account, as a mitigating factor, for the purpose of Article 83(2)(c) GDPR. As regards the remaining factors – Articles 83(2)(a), (b), (d), (g) and (k) – paragraph 178 of the Article 65 Decision makes it clear that the EDPB considered each of these factors to be aggravating.

9.90 Paragraph 174 of the Article 65 Decision makes it clear that the EDPB requires the DPC to apply the EDPB's Guidelines on calculation of fines[216] ("the **Fining Guidelines**") when calculating the amount of the administrative fine to be imposed in the within inquiry.

9.91 The Fining Guidelines firstly require the identification of a starting amount for further calculation of the fine on the basis of whether the infringement is classified as being of a low, medium or high degree of seriousness. Paragraph 52 of the Fining Guidelines clarify that this starting amount is to be determined by reference to the assessments that have been carried out pursuant to Articles 83(2)(a), (b) and (g) GDPR. The EDPB confirmed, in this regard, at paragraph 173 of the Article 65 Decision, that:

> *"Therefore, based on the evaluation of the factors under Article 83(2)(a), (b) and (g) GDPR, the EDPB takes the view that the infringement is of a high level of seriousness."*

[216] Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0, Adopted 12 May 2022

9.92 The EDPB concluded, at paragraph 174 of the Article 65 Decision, that:

> *"… the LSA should determine the starting amount for further calculation of the fine at a point between 20 and 100% of the applicable legal maximum."*

9.93 At paragraph 175 of the Article 65 Decision, the EDPB notes that:

> *"… after having evaluated the nature, gravity and duration of the infringement as well as the intentional or negligent character of the infringement and the categories of personal data affected, account must also be taken of the remaining aggravating and mitigating factors under Article 83(2) GDPR."*

9.94 It is important to note, in this regard, that, as clarified by paragraph 73 of the Fining Guidelines, each of the Article 83(2) criteria should only be taken into account once as part of the overall assessment of Article 83(2) GDPR. This means that, in the context of the assessments reflected in the Article 65 Decision, the only Article 83(2) criteria that remain to be taken into account, after the starting point for further assessment has been determined by reference to the assessments of Articles 83(2)(a), (b) and (g), are the assessments that were carried out by the EDPB by reference to Articles 83(2)(d) and (k) GDPR.

9.95 In this regard, the EDPB made it clear, at paragraph 176 of the Article 65 Decision, that:

> *"the factors referred to in Article 83(2) (d) and (k) GDPR are aggravating and should be attributed sufficiently heavy weight in the calculation of the administrative fine by the LSA."*

9.96 In addition to the above, I note that, further to Meta Ireland's Final Submissions, I concluded that the provision of the Additional Information ought to be taken into account, as a mitigating factor of light weight, for the purpose of Article 83(2)(c) GDPR.

9.97 I proposed, by way of the Annex, to impose an administrative fine of an amount falling within the range of €1.2 billion and €1.5 billion in respect of the infringement of Article 46(1) GDPR.

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

a. The purpose of the fine, which is to sanction the infringement of Article 46(1) that was found to have occurred;

b. The requirement for any fine to be effective. In this regard, the DPC notes that the fine proposed above reflects the circumstances of the case, as assessed by the EDPB in the Article 65 Decision, including both the specific elements of the infringement as well as those elements that relate to the controller which committed the infringement, namely its financial position. I note, in this regard, that the EDPB determined that the Infringement is of "*significant nature, gravity and duration*", committed with "*at least the highest degree of negligence*" and that Meta Ireland has a "*high degree of responsibility*". Furthermore, the EDPB did not identify any mitigating factors and, instead, identified two aggravating factors that determined ought to be attributed "*sufficiently heavy weight*". In terms of the requirement for me to take account of Meta Ireland's financial position, I have taken account of the very significant turnover of the undertaking of which Meta Ireland forms part, namely the Meta Platforms, Inc. group of companies (the DPC's assessment of the applicable turnover figure is detailed below). I note that I am required to take these particular matters into account not only by paragraph 177 of the Article 65 Decision but also by paragraph 414 of the EDPB's binding decision 1/2021. The combination of all of these factors (namely, the most serious classification for the purpose of calculating the starting point (assessed by reference to Articles 83(2)(a), (b) and (g) GDPR) with further adjustment to take account of two aggravating factors of "*sufficiently heavy weight*" (representing the EDPB's assessments of Articles 83(2)(d) and (k) GDPR) along with a very significant level of turnover) suggests that an administrative fine of an amount selected at a point extending beyond the mid-range of the scale identified by the EDPB in the Article 65 Decision ought to be imposed. This remains my view, notwithstanding my subsequent conclusion that the provision of the Additional Information ought to be taken into account as a mitigating factor for the purpose of Article 83(2)(c) GPDR, in circumstances where I concluded that only a light weight could be attributed to this factor;

c. The requirement for a genuinely deterrent effect, in terms of discouraging both Meta Ireland and others from committing the same infringement in the future;

d. The requirement for any fine to be proportionate and to not exceed what is necessary to achieve the stated objective (as recorded at a., above). The DPC considers that the fine proposed is proportionate to the circumstances of the case, taking into account

the gravity of the infringements and all of the elements that may lead to an increase (aggravating factors) or decrease (mitigating factors) of the initial assessment as well as the significant turnover of the undertaking concerned, as assessed by the EDPB in the Article 65 Decision. The fine also takes account of the fact that it will be imposed in addition to orders requiring Meta Ireland to take action to bring its processing into compliance. As noted by the EDPB, as part of its assessment of the Article 83(2)(k) criterion, "*it can be inferred that transferring the data to the US in a way that infringes the GDPR is inextricably linked to the provision of the service to EU/EEA individuals*". The EDPB further noted Meta Ireland's submissions that "*the suspension order proposed by the IE SA would have 'severe consequences' for Meta IE and 'would clearly have a devastating impact on FIL's business, revenue and employees'*" and concluded that this suggested that "*a considerable part of its profits derived from the provision of the service in the EU arise from the breach of the GDPR*." As noted above, I have already taken account of the EDPB's Article 83(2)(k) assessment as an aggravating factor with sufficiently heavy weight. By the same token, I cannot ignore Meta Ireland's submissions that the suspension order would have "*severe consequences*" for its business. I accept that the suspension order will likely have adverse consequences for Meta Ireland. I also accept that, while the orders to bring processing into compliance are being made for the purpose of bringing about the remedial action required to address the Infringement, I cannot ignore the negative financial consequences that will likely flow from the action that might be required to be taken by Meta Ireland in order to achieve compliance with the orders ("the **Financial Consequences**"). In these circumstances, I have taken account of the Financial Consequences by applying a reduction to the overall quantum of the administrative fine in order to ensure that the fine is proportionate to all of the circumstances of the case, as required by Article 83(1) GDPR. As set out at paragraph b., above, my view, following the completion of the Article 83(2) GDPR assessment (which is the basis upon which the amount of the administrative fine must be determined) was that an administrative fine of an amount selected at a point extending beyond the mid-range of the scale identified by the EDPB in the Article 65 Decision ought to be imposed. In terms of the reduction that ought to be applied to that conclusion, for the purpose of taking account of the Financial Consequences and ensuring that the fine to be imposed is proportionate, in accordance with Article 83(1) GPDR, I consider that a reduction the equivalent to a mitigating factor of moderate weight must be applied, when

determining the range of the administrative fine proposed above. That reduction has been reflected in the fining range proposed at paragraph 9.97, above.

Meta Ireland's Final Submissions on Article 83(1) GDPR

9.99 The manner in which the DPC has determined that the proposed fining range is "*effective, proportionate and dissuasive*" for the purpose of Article 83(1) GDPR is set out in paragraph 9.98, immediately above. I will now consider the submissions furnished by Meta Ireland, in response to that assessment (as it appeared in the Annex).

9.100 By way of Section 5 of the Final Submissions, Meta Ireland has submitted[217] that the DPC has not been instructed, by the EDPB, to "*have regard to the EDPB's assessment under Article 83(1) when deciding what level of fine complies with Article 83(1), in the operative or any other part of the Article 65 Decision*." Meta Ireland has further submitted[218], in this regard, that:

> *"5.10 Meta Ireland respectfully submits that, insofar as the DPC purports to carry out an assessment under Article 83(1) GDPR in the Annex, this assessment is erroneous insofar as it treats the DPC as bound by the assessment carried out by the EDPB under Article 83(1) for the purpose of determining whether an administrative fine ought to be imposed, rather than the quantum of the fine. The EDPB deliberately has not instructed the DPC to have regard to this assessment in the determination of the quantum of the administrative fine to be imposed."*

9.101 To be clear about the position, the DPC has carried out its own assessment of the extent to which the fining range proposed above achieves compliance with the requirements of Article 83(1) GDPR. That assessment was outlined in the Annex and is now set out at paragraph 9.98, above.

9.102 Meta Ireland has further submitted[219] that "*it is not possible to ascertain … how the DPC fixed the fining range within the parameters set by the EDPB, in the exercise of the limited discretion the DPC considers has been left to it by the EDPB*". Meta Ireland has submitted[220] that this has "*significantly interfered with*" its ability to make meaningful submissions. I disagree that this is the case. As is evident from the extensive analysis set out above (which was also included in the Annex), the DPC has clearly identified how it calculated the fining range by reference to

[217] The Final Submissions, Section 5, paragraph 5.7
[218] The Final Submissions, Section 5, paragraph 5.10
[219] The Final Submissions, Section 5, paragraph 5.19
[220] Ibid.

the Article 83(2) assessments. Furthermore, the manner in which the relevant factors have been taken into account, as mitigating or aggravating factors, as well as the weight that has been attributed to each one has been clearly addressed. The analysis also explains how the DPC assessed the proposed fining range to be "*effective, proportionate and dissuasive*" for the purpose of Article 83(1) GDPR. This approach is in line with the DPC's obligation to provide reasons for its decisions. While the DPC is required to explain how it arrived at the level of a proposed fine, it is not required to apply such specificity so as to allow a controller or processor to make a precise mathematical calculation of the expected fine[221].

9.103 I further note Meta Ireland's submission[222] that:

> "*It appears from sub-paragraph (b) of pages 21-22 of the Annex, regarding the requirement for any fine to be effective, that the DPC considered that the EDPB's assessment of the factors provided for in Article 83(2) GDPR "suggests that an administrative fine of an amount selected at a point extending beyond the mid-range of the scale identified by the EDPB in the Article 65 Decision ought to be imposed". In this regard, to the extent the consideration of the issues in this sub-paragraph (b) of the Annex has led to an increase in the administrative fine, any such increase should be discounted on the basis that the DPC has, contrary to the Draft Fining Guidelines, counted these issues twice*."

9.104 For the avoidance of doubt, the DPC has not taken any of the Article 83(2) assessments into account twice. This is self-evident from the analysis set out above and, in particular, the analysis set out at paragraph 9.98, above.

9.105 Meta Ireland has further submitted[223] that:

> *"… the DPC retains the discretion under Article 83(1) GDPR to impose a fine lower than the starting amount for further calculation for the fines specified by the EDPB in the Article 65 Decision*."

9.106 I agree that this is a correct assessment of both the Article 65 Decision as well as the Fining Guidelines. Notwithstanding Meta Ireland's submissions, I remain of the view that the fining range proposed above is "*effective, proportionate and dissuasive*" for the purpose of Article

[221] See, by analogy, HSBC Holdings plc and Others v Commission, T-105/17, ECLI:EU:T:2019:675, paragraphs 336 – 354.
[222] The Final Submissions, Section 5, paragraph 5.21
[223] The Final Submissions, Section 5, paragraph 5.28

83(1) GDPR. I have already detailed, above, why I consider this to be the case. By way of summary of the key factors:

a. The EDPB has determined that the DPC must apply the Fining Guidelines when calculating the quantum of the administrative fine;

b. The EDPB has further determined that the starting point for further calculation should be determined at a point between 20% and 100% of the applicable legal maximum. This is the highest of the three possible starting ranges for further calculation set out in the Fining Guidelines;

c. Based on the evaluation of the factors under Article 83(2)(a), (b) and (g) GDPR, the EDPB determined that the Infringement is of a high level of seriousness;

d. Further to its assessments of the factors arising pursuant to Articles 83(2)(d) and (k) GDPR, the EDPB concluded that the relevant factors are aggravating and should be attributed "sufficiently heavy weight" in the calculation of the administrative fine;

e. The EDPB did not identify the existence of any mitigating factors;

f. The DPC took account, as a mitigating factor of light weight for the purpose of the Article 83(2)(c) assessment, of the Additional Information that has been provided to Users by Meta Ireland;

g. The DPC further applied a significant reduction to the outcome of the Article 83(2) assessment, in order to take account of the Financial Consequences for the purpose of ensuring that the fining range was "*effective, proportionate and dissuasive*", as required by Article 83(1) GDPR. The reduction applied, in this regard, is equivalent to a mitigating factor of moderate weight.

9.107 In the circumstances, the DPC is satisfied that the proposed fining range reflects the individual circumstances of this particular case, as required by Articles 83(2) and 83(1) GDPR.

9.108 As regards Meta Ireland's attempted reliance on the view that was expressed in the Draft Decision, that "*the Data Transfers were being effected, in good faith, under and by reference to transfer mechanisms provided for at law*", it is clear, from the EDPB's assessment of the

character of the Infringement for the purpose of Article 83(2)(b) GDPR, that the EDPB does not agree with this view. The DPC is obliged, pursuant to Article 65(6) GDPR, to adopt (this) final decision "*on the basis of*" the Article 65 Decision. In the circumstances, I cannot take this matter into account, as a mitigating factor, when calculating the amount of the fine to be imposed.

9.109 Under the heading of "*effectiveness*", Meta Ireland has submitted[224] that "*there is no basis to conclude that an administrative fine of the magnitude proposed … is appropriate or necessary for reasons of effectiveness. This is entirely inconsistent with the views expressed by the DPC previously in this Inquiry*."

9.110 It is not disputed that the views expressed by the DPC in the Draft Decision are not consistent with the outcome recorded in this Decision. It stands to reason that, in giving effect to the binding determination of the EDPB, that the DPC must amend the positions previously reflected in the Draft Decision that are not consistent with the determinations made by the EDPB so that this Decision may be adopted "*on the basis of*" the Article 65 Decision, as required by Article 65(6) GDPR.

9.111 Having taken account of Meta Ireland's Final Submissions, I remain of the view that an administrative fine of an amount falling with the range of €1.2 billion and €1.5 billion ought to be imposed in respect of the infringement of Article 46(1) GDPR, for the reasons outlined in paragraph 9.98, above.

Assessment of the Undertaking Concerned and the Applicable Fining "Cap"

9.112 The infringement of Article 46(1) GDPR is subject to the higher fining "cap" set out in Article 83(5) GDPR, as follows:

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

[224] The Final Submissions, Section 5, paragraph 5.31

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

…"

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

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

9.114 Accordingly, when considering a respondent's status as an undertaking, the GDPR requires me to do so by reference to the concept of 'undertaking', as that term is understood in a competition law context. In this regard, that the 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*[225]"

9.115 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[226].

9.116 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

[225] *Höfner and Elser v Macrotron GmbH* (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161 §21
[226] *Akzo Nobel and Others v Commission*, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, § 58 - 61

calculated by reference to the turnover of the undertaking as a whole, rather than the turnover of the controller or processor concerned.

9.117 In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case[227].

9.118 The CJEU has, however, established[228] that, where a parent company has a 100% shareholding in a subsidiary, it follows that:

a. the parent company is able to exercise decisive influence over the conduct of the subsidiary; and

b. a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

9.119 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[229].

9.120 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[230]. 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,*

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

[228] Akzo Nobel and Others v Commission, (C-97/08 P, judgment delivered 10 September 2009)

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

[230] 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

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 …[231]"

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

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

Application of the above to the within inquiry

9.123 At paragraph 177 of the Article 65 Decision, the EDPB determined as follows:

"*When calculating the final amount of the fine, the [DPC] should use the total worldwide annual turnover of the undertaking concerned for the preceding financial year, i.e. the worldwide annual turnover of all the entities composing the single undertaking.* ***In the present case, this is the consolidated turnover of the group of companies headed by Meta Platforms, Inc.*** *On the notion of 'preceding financial year', the event from which the preceding financial year should be considered is the date of the final decision taken by the LSA pursuant to Article 65(6) GDPR*." [emphasis added]

9.124 Applying the above to Article 83(5) GDPR, I firstly note that, in circumstances where the fine is being imposed on an "undertaking", a fine of up to 4% of the total worldwide annual turnover of the preceding financial year may be imposed. I note, in this regard, that Meta Platforms Inc. reported the generation of revenue in the amount of $116.61 billion for the year ending

[231] 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)

31 December 2022.[232] That being the case, the administrative fine proposed above does not exceed the applicable fining "cap" prescribed by Article 83(5) GDPR.

9.125 For the sake of completeness, I acknowledge Meta Ireland's submission[233] that it considers the approach taken above, further to the instructions of the EDPB, "*constitutes an error of law*". I am unable to take account of Meta Ireland's views, in this regard, in circumstances where the DPC is subject to the clear and unequivocal determination of the EDPB, as recorded at paragraph 177 of the Article 65 Decision, that requires the DPC, amongst other things, to use the consolidated turnover of the group of companies headed by Meta Platforms, Inc. when calculating the final amount of the fine.

10. SUMMARY OF FINDINGS AND CONCLUSION

Summary of Findings and Decision

10.1 Having regard to the provisions of Section 111 of the 2018 Act, and for the reasons set out in this Decision, I find that:

(i) US law does not provide a level of protection that is essentially equivalent to that provided by EU law;

(ii) Neither the 2010 SCCs nor the 2021 SCCs can compensate for the inadequate protection provided by US law;

(iii) Meta Ireland does not have in place supplemental measures which compensate for the inadequate protection provided by US law; and,

(iv) It is not open to Meta Ireland to rely on the derogations provided for at Article 49(1) GDPR, or any of them, when making the Data Transfers.

10.2 Accordingly, I find (and it is my decision that), in making the Data Transfers, Meta Ireland is infringing Article 46(1) GDPR.

---

[232] https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx#:~:text=Revenue%20%E2%80%93%20Revenue%20was%20%2432.17%20billion,and%20full%20year%202022%2C%20respectively.

[233] As set out in the letter dated 8 May 2023, from Meta Ireland's legal representatives to the DPC

10.3 I am satisfied (and I so decide) that it is appropriate that I should exercise corrective powers in respect of Meta Ireland, as the relevant Controller, as follows:

(i) I make an order, pursuant to Article 58(2)(j) GDPR, to require Meta Ireland to suspend the Data Transfers in accordance with the timeline outlined below ("the **Suspension Order**");

(ii) further to the determination of the EDPB set out at paragraph 267 of Article 65 Decision, I make an order pursuant to Article 58(2)(d) GDPR to require Meta Ireland to bring its processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, within 6 (six) months following the date of notification of this Decision to Meta Ireland; and

(iii) I impose, pursuant to Article 58(2)(i) GDPR, an administrative fine in the amount of €1.2 billion. I consider that an administrative fine of this amount reflects the assessments of Article 83(2) and 83(1) GPDR that are recorded in Section 9, above.

Timeline for compliance with the Suspension Order

10.4 For the purpose of this Section 10, "the **Commencement Date**" shall be understood as meaning the date corresponding to the later in time of the following events: (i) the date on which the period allowed for an appeal against this Decision under Section 150 of the 2018 Act expires; and (ii) the date on which the period allowed for the bringing of an application for annulment of the Article 65 Decision under Article 243 TFEU expires.

10.5 The Suspension Order will take effect on a date 12 (twelve) weeks from the Commencement Date.

10.6 During the said period of 12 weeks, Meta Ireland is invited to make submissions to the DPC outlining, with precision:

(i) how it will implement the suspension in a manner consistent with its obligations to Users, to include its obligations under and by reference to Chapter III of the GDPR; and,

(ii) how, and when, it will communicate its plans to Users.

10.7 Such submissions shall be made to the DPC not later than 4 weeks after the Commencement Date.

10.8 On receipt of such submissions, the DPC will engage with Meta Ireland and will endeavour to agree the terms of its implementation plan within a further period of 4 weeks, commencing on the date of receipt of Meta Ireland's submissions.

10.9 Upon agreement of such implementation plan, Meta Ireland will be afforded a further and final period of 4 weeks to give effect to same such that the Data Transfers shall be suspended no later than 12 weeks from the Commencement Date.

10.10 For the avoidance of doubt, if Meta Ireland fails to submit an implementation plan to the DPC within the time period noted (or at all) and/or the terms of an implementation plan cannot be agreed between the parties (whether within the time period noted, or at all), Meta Ireland will nonetheless be bound to give effect to the Suspension Order no later than 12 weeks from the Commencement Date.

Other Matters

Scope of application of the final decision

10.11 This Decision will bind Meta Ireland only. It is clear, however, that the analysis in this Decision exposes a situation whereby *any* internet platform falling within the definition of an electronic communications service provider subject to the FISA 702 PRISM programme may equally fall foul of the requirements of Chapter V GDPR and the EU Charter of Fundamental Rights regarding their transfers of personal data to the USA. This point was raised by the DPC before the Irish High Court and the CJEU when it raised questions as to the validity of the SCC instruments specifically as a mechanism underpinning transfers to the United States. In the event, the CJEU upheld the validity of the SCCs as a legal instrument, emphasising the need to undertake a case-by-case assessment to determine whether, in any given case, data transfers to a third country conducted under their terms are lawful or not. In the circumstances, and notwithstanding the findings made by the CJEU in the Judgment in relation to US law, it is not open to the DPC to make an order suspending or prohibiting transfers to the United States generally.

Right of an effective remedy

10.12 Meta Ireland has the right of an effective remedy as against this Decision, the details of which have been provided separately.

<u>This Decision is addressed to</u>:

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

Dated the 12th day of May 2023

Decision-Maker for the Commission:

_____

Helen Dixon
Commissioner for Data Protection

SCHEDULE

EDPB Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted 13 April 2023