



THE HIGH COURT

COMMERCIAL

Record No.: 2025/248 MCA

IN THE MATTER OF SECTION 142 AND SECTION 150

OF THE DATA PROTECTION ACT 2018

Between:

**TIKTOK TECHNOLOGY LIMITED and TIKTOK INFORMATION
TECHNOLOGIES UK LIMITED**

Appellants

And

DATA PROTECTION COMMISSION

Respondent

JUDGMENT of Mr Justice Rory Mulcahy delivered on 3 June 2026

CONTENTS

Introduction.....	3
The transfers.....	8
The General Data Protection Regulation (GDPR).....	9
Data Protection Act 2018.....	20
The inquiry.....	24
The Decision	44
The Data Transfer Assessments	50
Scope of the appeal	56
Nature of the Inquiry.....	65
Grounds of appeal	69

Ground 3 – Errors of law	71
The decision in <i>Schrems II</i>	73
Alleged misinterpretation of the GDPR	79
<i>Arguments</i>	79
<i>Discussion</i>	81
Alleged reversal of burden of proof	90
<i>Arguments</i>	90
<i>Discussion</i>	92
Alleged requirement to carry out risk assessment	95
<i>Arguments</i>	95
<i>Discussion</i>	98
Overall conclusion on Ground 3	101
Grounds 1 – Breach of fair procedures	102
Failure to put adverse findings to TikTok	104
<i>Arguments</i>	104
<i>Discussion</i>	107
Failure to have regard to submissions made	115
<i>Arguments</i>	115
<i>Discussion</i>	118
Failure to adequately assess Project Clover	121
<i>Arguments</i>	121
<i>Discussion</i>	122
Impermissible amendment of temporal scope	124
<i>Arguments</i>	124
<i>Discussion</i>	125
Failure to make the file available	126
<i>Arguments</i>	126
<i>Discussion</i>	128
Ground not pleaded	129
Overall conclusion on Ground 1	130
Grounds 2 and 10	130
Alleged errors in assessment	130
<i>Arguments</i>	132
<i>Discussion – errors in assessment of Chinese law evidence</i>	133
<i>Discussion – errors in assessment of Project Clover</i>	145

Overall conclusions on Ground 2 and 10.....	155
Ground 11 – Error in making the corrective orders	156
<i>Arguments – ground 11</i>	156
<i>Discussion – ground 11</i>	158
Overall conclusion on Ground 11	160
Ground 5 – misrepresentation and misapplication of Article 13(1)(f).....	161
<i>Arguments</i>	164
<i>Discussion</i>	166
Overall conclusion on Ground 5	169
Appeal against fines.....	169
Ground 6 – failure by the DPC to establish that TikTok was negligent	170
<i>Arguments</i>	173
<i>Discussion</i>	174
Overall conclusion on Ground 6	177
Summary of conclusions.....	178
Proposed Order	181

Introduction

1. The General Data Protection Regulation (Regulation (EU) 679/2016), generally known as the GDPR, confers significant rights on all EU citizens in respect of their personal data, including rights to clear information, rights of access, rights of rectification, and rights of redress. Its territorial scope is the EU (and EEA, the GDPR having been formally incorporated into the EEA Agreement on 6 October 2018).
2. Controllers and processors of personal data may only transfer that personal data outside the EEA when the data will be subject to essentially equivalent levels of protection in the third countries to which the data is transferred to that guaranteed within the EEA.
3. This appeal concerns, at its heart, the scope of the obligations imposed on controllers of personal data when transferring personal data outside the EEA.
4. The appellant (“**TikTok**”) challenges a finding by the respondent (“**the DPC**”) that TikTok had failed to fulfil its obligation when transferring certain personal data of its users

to China, and that it must stop transferring that data until it is in a position to comply with the requirements of the GDPR. TikTok contends that the DPC has misunderstood the nature of the obligations imposed by the GDPR.

5. On 14 September 2021, the DPC commenced an inquiry (“**the Inquiry**”) into TikTok in accordance with section 110 of the Data Protection Act 2018 (“**the 2018 Act**”). The DPC is the State’s supervisory authority for the purpose of the GDPR.

6. Following a lengthy investigation, and having consulted with other supervisory authorities in accordance with Article 60 of the GDPR, the DPC issued its decision on 30 April 2025 (“**the Decision**”). The Decision for the first time defined the temporal scope of the Inquiry as relating to data transfers taking place from 29 July 2020 until 17 May 2023 (“**the temporal scope**”). In the Decision, the DPC found that TikTok had infringed Article 46(1) of the GDPR by failing to ensure that personal data of its users within the European Economic Area (“**EEA Users**”) which was transferred outside the EEA, in this case by being made available by remote access to personnel based in China (“**the data transfers**”), was afforded a level of protection essentially equivalent to that provided within the European Union (“**EU**”) during the Inquiry’s temporal scope. The particular concern identified by the DPC was that the regulation of public authority access to personal data pursuant to identified Chinese laws (“**the relevant Chinese laws**”) diverged materially from the protections conferred by the GDPR and TikTok had not established that the relevant Chinese laws would not apply to the data transfers.

7. The Decision also found that TikTok had breached Article 13(1)(f) of the GDPR by failing to provide required information on the data transfers to data subjects from 29 July 2020 to 1 December 2022.

8. The DPC imposed administrative fines totalling €530 million pursuant to Article 58(2)(i) of the GDPR. The second appellant (“**TikTok UK**”) has been joined to these proceedings on the basis that it is the party which will ultimately be responsible for paying any such administrative fine. The DPC disputes its standing as a party in these proceedings though it is not necessary to address that issue for the purpose of this judgment.

9. In addition to the administrative fines, the DPC made orders pursuant to Article 58(2)(j) of the GDPR requiring TikTok to suspend the data transfers (“**the suspension order**”) and to bring the manner in which it processed personal data into line with the GDPR “*in the manner described in*” the Decision (“**the processing order**”) (together “**the corrective orders**”).

10. The Decision can, therefore, be considered as comprising four relevant parts: (1) a decision that TikTok had infringed Article 46(1) of the GDPR between 29 July 2020 and 17 May 2023; (2) a decision that TikTok had infringed Article 13(1)(f) of the GDPR between 29 July 2020 and 1 December 2022; (3) a decision to impose the corrective orders; and (4) a decision to impose administrative fines for the infringements.

11. By originating notice of motion issued on 27 May 2025, TikTok appealed the Decision pursuant to section 142 and, if necessary, section 150 of the 2018 Act.

12. In the affidavit of Elaine Fox, Head of Privacy, Europe and Head of Ireland at TikTok, TikTok identified a total of eleven grounds of appeal. As discussed in further detail below, the grounds are directed to each of the constituent parts of the Decision. Many of the eleven grounds comprise a number of individual grounds.

13. It is worth observing at this point that a central feature of TikTok’s position that it had complied (and continues to) with the requirements of Article 46 is that it employs what is termed the “*remote access solution*”, whereby personal data processed in China is stored outside China and remotely accessed from China. TikTok’s position is that as a matter of Chinese law, any entitlement of the Chinese authorities to access personal data pursuant to the relevant Chinese laws is subject to the territoriality principle, and that the Chinese authorities have no power to access data stored outside of China. It contends that the personal data the subject of the Inquiry, although remotely accessed (and accessible) in China, is at all times stored outside China and therefore outside the jurisdiction of Chinese authorities. In substance, the DPC accepted that by virtue of the territoriality principle, data stored outside China is not subject to the relevant Chinese laws and therefore not at risk of a lower level of protection than that guaranteed in the EU. However, it concluded that TikTok had not addressed the application of the relevant Chinese laws to personal data which was actually being processed *in* China.

14. The institution of proceedings automatically stayed the requirement to pay the administrative fines, by operation of section 142 of the 2018 Act. The corrective orders, however, had immediate effect, and accordingly, TikTok sought a stay on those orders. Following a four-day hearing between 7 and 10 October, I granted TikTok a stay on implementation of the corrective orders, subject to certain conditions, in a judgment dated 13 November 2025 ([2025] IEHC 619) (“**the stay judgment**”). Some of the factual content in this judgment has already been rehearsed in the stay judgment. The DPC sought and obtained leave to appeal from that judgment to the Supreme Court, and an appeal was heard between 17 and 19 February 2026. By judgment dated 30 April 2026 ([2026] IESC 27), the Supreme Court decided to continue the stay pending the determination of these proceedings in the High Court.

15. On 12 February 2026, TikTok issued a motion seeking a similar order to one obtained in the stay application, to protect the confidentiality of information it had provided to the DPC in confidence during the Inquiry. The application was heard on 20 February 2026, and I made the order sought in similar terms to the earlier order, for similar reasons (see §10 - §13 of the stay judgment). During the course of the hearing, some of the information over which protection had been provided was referred to in open court, either because TikTok elected to do so, or because it became apparent that the protection was not required in relation to that information. I have referred in this judgment to some of the material identified as confidential by TikTok. I provided this judgment to the parties in draft form to enable the parties to identify any information contained within it which they wished to apply to have redacted. Very limited redactions were proposed by TikTok in order to continue to protect confidential information the disclosure of which could undermine its security measures. I am satisfied that the making of the redactions proposed is consistent with the confidentiality orders previously made and I have, accordingly, applied those limited redactions to this judgment.

16. These proceedings were heard over ten days between 3 and 19 March 2026. During the course of the hearing, the parties indicated that they were in agreement that certain of the legal issues raised in the appeal regarding the administrative fines might benefit from a preliminary reference to the CJEU pursuant to Article 267 of the Treaty on the Functioning of the European Union (“**TFEU**”). In this regard, it should be noted that Ground 6 of the appeal related to the DPC’s entitlement to impose administrative fines, and the remaining

grounds, Grounds 7, 8, and 9, related to the calculation of those fines. Certain of the legal issues between the parties are also the subject of pending annulment proceedings before the General Court of the CJEU, Case C-97/23P, *WhatsApp v EDPB*, and it was contended that the duty of sincere co-operation at Article 4(3) of the TFEU might necessitate a reference in those circumstances. The parties engaged regarding the questions which they considered should be referred, and a document setting out their respective positions was provided on 18 May 2026. The parties agreed the terms of some questions and made separate proposals in relation to others.

17. In light of this development, I suggested to the parties that I could deliver separate judgments, one on the grounds of appeals relating to the administrative fines (Grounds 6, 7, 8 and 9), and one on all the other grounds. The parties were amenable to that approach. However, having considered the matter further, and in particular having considered the issues which the parties suggest should be referred to the CJEU, it appears to me sensible to deal in this judgment with all issues concerning whether the DPC was entitled to impose administrative fines *at all* (*i.e.* Ground 6), which I consider can be addressed without the necessity for a reference to the CJEU, and to leave over for a further judgment the grounds relating to how any such fine should be calculated, which do give rise to some issues where a reference would be appropriate.

18. This, accordingly, is the first of two intended judgments on the substantive appeal. A second judgment (“**the fines judgment**”), dealing with Grounds 7, 8 and 9 of the appeal will follow in early course.

19. At the time of hearing, judgment was awaited in a trial of preliminary issues in a separate appeal against a decision of the DPC. It was anticipated that the judgment would address the scope of the appeal provided for under the 2018 Act, and accordingly the parties did not address that issue in detail but set out a summary of their positions in their written submissions. It was agreed that short further submissions would be provided once judgment was delivered. Those further submissions were provided by TikTok and the DPC respectively on 7 and 14 May 2026 in light of the judgment in *LinkedIn v DPC* [2026] IEHC 235, which is discussed below.

20. Having regard to the multiplicity of issues raised in this appeal, I propose to address each ground separately, setting out the arguments and the analysis in relation to each in turn. There are, however, some issues which could cut across multiple grounds, such as the standard of review applicable to decisions of the DPC in a statutory appeal, and the nature of the inquiry and sanctions provided for in the GDPR. I will deal with those overarching questions before addressing the individual grounds. Before doing so, however, I propose to identify the relevant provisions of the GDPR and the 2018 Act and then set out in a little detail the history of the Inquiry. It might be helpful first to explain the nature of the transfers the subject of that Inquiry.

The transfers

21. The TikTok Platform is a global entertainment platform that was launched in the EU in 2017 and in the EEA in 2018. It is available in more than 150 countries via an application that can be downloaded on mobile phones and tablets, VR headsets and other smaller distribution channels as well as via a web browser. The TikTok Platform enables its users (individuals that view and/or engage with content on the TikTok Platform, referred to as “**Users**”) and creators (TikTok Users who create and/or post videos, audio, images and other content on the TikTok Platform, referred to as “**Creators**”) to create, share and watch video content.

22. TikTok collects data from its users which is stored in data centres. A subset of that data can be accessed remotely by personnel of certain China Group Entities (“**CGEs**”), being a list of identified companies associated with TikTok, for the purpose of carrying out a variety of processes which TikTok says are essential to its operations. The access is subject to strict conditions. TikTok accepts that some of the data which is remotely accessed is personal data within the meaning of the GDPR. It also accepts that this remote access constitutes a transfer for the purpose of the GDPR. TikTok calls the data which can be accessed remotely ‘allowable’ data. Allowable data consists of (i) inter-operable data, which is data needed for the TikTok platform to operate globally; (ii) public data, a type of inter-operable data which is publicly available and accessible by anyone on the TikTok platform, and (iii) aggregated data, allowable data which is compiled and expressed in a summary way.

23. As set out below, during the course of the Inquiry, TikTok added additional protections to the data which can be accessed in China as part of a suite of measures it calls Clover or Project Clover.

24. In the context of the stay application, TikTok explained in a little detail the purposes for which the transferred data is used in China and the business processes which would be affected if it was not permitted to transfer any data to China. These include product and feature updates, algorithm updates, bug identification and issues resolution, and prevention and resolution of platform and services outages. The key business groups involved are the e-commerce group, the monetisation group, the TikTok Short Video group and the TikTok live group. As set out in the stay judgment, many thousands of CGE employees are engaged in the processing of EEA user data for these purposes. The volume of data involved is clearly very significant.

The General Data Protection Regulation (GDPR)

25. Recital 1 of the GDPR recognises that the protection of natural persons in relation to the processing of personal data is a fundamental right and references Article 8(1) of the Charter of Fundamental Rights of the European Union (“**the Charter**”) and Article 16(1) of the TFEU, each of which provides that everyone has the right to the protection of personal data concerning him or her.

26. Recital 4 provides that:

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and 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.

27. Recital 26 refers to the scope of the GDPR and, in particular, its application to information about “*identified or identifiable natural persons*”:

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

28. Recital 60 relates to transparency obligations:

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

29. Recital 74 concerns the responsibilities of controllers:

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective

measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

30. Recital 101 concerns the transfer of data outside the EU:

Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

31. Recitals 124 to 126 discuss the role of supervising authorities and the competence of lead supervising authorities.

32. Recital 129 relates to the tasks and powers of supervisory authorities. It includes the following:

... The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every

person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned ...

33. Recital 143 refers to the entitlement to a judicial remedy.

Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State....

34. Article 4 of the GDPR contains a number of definitions relevant for the purpose of these proceedings:

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

(2) *‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

...

(5) *‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*

...

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

(8) *‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller...*

35. Article 5(1) of the GDPR sets out the principles which apply to all processing of personal data: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. Article 5(2) provides that the principle of accountability should apply to all of the foregoing, *i.e.* that a data processor should be able to demonstrate compliance with all of the foregoing:

1. Personal data shall be:

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

- b. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*
- c. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
- d. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*
- e. *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*
- f. *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

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

36. The requirement for accountability, or responsibility, is also found in Article 24(1):

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational

measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

37. Chapter V relates to the cross-border transfer of data, that is transfers outside the EEA. The overriding requirement is that the rights guaranteed by the GDPR are not compromised by any such transfer of personal data, that data is afforded an equivalent level of protection in a third country as it would have within the EEA. Thus, Article 44 provides:

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

38. Articles 45 and 46 provide alternative mechanisms for ensuring equivalent protection. Article 45 provides for the making of adequacy decisions by the European Commission. Where the Commission has determined that adequate protection is provided in a third country, and makes a decision to that effect, then transfers to that country do not require further authorisation.

39. Where, as here, there is no adequacy decision under Article 45, transfers are still permitted without specific authorisation where the data processor satisfies the requirements of Article 46:

- 1. In the absence of a decision pursuant to Article 45(3), 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.*

2. *The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:*
- a) a legally binding and enforceable instrument between public authorities or bodies;*
 - b) binding corporate rules in accordance with Article 47;*
 - c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);*
 - d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);*
 - e) 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; or*
 - f) 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.*

40. Commission decisions under Article 45 and 46(2)(c) were the subject of the leading cases in Case C-362/14, *Schrems v DPC* (“**Schrems I**”) and Case C-311/18, *DPC v Facebook Ireland* (“**Schrems II**”).

41. Chapter VI of the GDPR deals, *inter alia*, with the decision-making functions of supervisory authorities. Pursuant to Article 51, each member state is required to designate at least one supervisory authority responsible for monitoring the application of the GDPR. Article 56 sets out the competencies of a supervisory authority. Article 56(1) provides:

Without prejudice to Article 55, 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.

42. Article 60 sets out the co-operation procedure between supervising authorities when, *inter alia*, investigating a complaint. Sub-articles 1 to 3 concern obligations in relation to the sharing of information. These include, at sub-article 3, an obligation on a lead supervising authority (“LSA”) to provide draft decisions to other supervisory authorities concerned (“SACs”) for their opinion and to “*take due account of their views*”. Other SACs may provide reasoned objections to any such draft decision. If agreement cannot be reached on those objections, a consistency mechanism is provided at sub-article 4, whereby any disagreement can be referred to the European Data Protection Board (“EDPB”) for resolution. A decision of the EDPB pursuant to Article 65 of the GDPR is binding upon the supervisory authorities. The EDPB is established by Article 68(1) of the GDPR as a union body with legal personality. It is comprised of the heads of at least one supervisory authority from each member state. If there are no reasoned objections, the LSA and SACs shall be deemed to be in agreement with the draft decision and “*shall be bound by it*”.

43. Article 78 of the GDPR requires that member states provide effective remedies regarding decisions of supervisory authorities:

1. *Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.*
2. *Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.*
3. *Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.*
4. *Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.*

44. Article 83 sets out the conditions for imposition of administrative fines:

1. *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*
2. *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
 - a. *the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
 - b. *the intentional or negligent character of the infringement;*
 - c. *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
 - d. *the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
 - e. *any relevant previous infringements by the controller or processor;*
 - f. *the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
 - g. *the categories of personal data affected by the infringement;*
 - h. *the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
 - i. *where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
 - j. *adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*
 - k. *any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*

3. *If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*
4. *...*
5. *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
 - a. *the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;*
 - b. *the data subjects' rights pursuant to Articles 12 to 22;*
 - c. *the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;*
 - d. *any obligations pursuant to Member State law adopted under Chapter IX;*
 - e. *non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).*
6. *Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, 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.*
7. *...*
8. *The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.*
9. *Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities.²In any event, the fines imposed shall be effective, proportionate and dissuasive.³Those Member States*

shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Data Protection Act 2018

45. On the face of the Decision , it notes that the inquiry was commenced of the DPC's own volition pursuant to s. 110 of the 2018 Act. The decision itself was then made pursuant to section 111 of same, and pursuant to Art 60 of the GDPR. Section 111 provides:

- (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 processor 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.*

46. Accordingly, where the DPC concludes that there has been an infringement, it is obliged to consider whether to exercise a corrective power.

47. Regarding the draft decision which was circulated to the SACs, the Decision (at §5) states that it was submitted to the SACs in accordance with Article 4(22) and 60(3) of the GDPR. A draft decision is provided for in section 113 of the Act:

(1) This section applies to a complaint in respect of which the Commission is the lead supervisory authority.

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

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

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

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

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

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

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

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

(i) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and

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

(5) The Commission, in making its decision under subsection (4), shall have due regard to the decision as to the envisaged action to be taken in relation to the controller or processor included in the Commission's draft decision under subsection (2)(a) or, as the case may be, its revised draft decision under Article 60.

- (6) The actions referred to in subsection (4)(b) include any or all of the following:*
- (a) the serving on the controller or processor concerned of an enforcement notice, requiring it to do one or more than one of the following:*
 - (i) comply with the data subject's request to exercise his or her rights pursuant to a relevant enactment;*
 - (ii) where the enforcement notice is given to the controller, communicate a personal data breach to the data subject;*
 - (iii) rectify or erase personal data or restrict processing pursuant to Article 16, 17 or 18, and, in respect of that action, to comply with Article 19 and, where applicable, Article 17(2);*
 - (aa) the issuing of a reprimand to the controller or processor concerned;]*
 - (b) the taking of such other action in respect of the complaint as the Commission considers appropriate.*

(7) The Commission—

- (a) where it makes a decision referred to in subsection (4)(a)(ii), shall exercise the corrective power concerned, ...*

48. Notably, neither Article 60 of the GDPR, nor section 113 of the 2018 Act suggest that there is any obligation to provide a draft decision to the parties to an inquiry.

49. Section 115(1) of the Act states:

(1) For the purposes of exercising a corrective power under section 111, 112 or 113, the Commission may do either or both of the following:

- (a) subject to Chapter 6, decide to impose an administrative fine on the controller or processor concerned;*

- (b) exercise any other corrective power specified in Article 58(2).*

(2) Without prejudice to the generality of subsection (1)(b), the Commission may, for the purposes of exercising a power referred to in that provision, serve on the controller or processor concerned an enforcement notice requiring it to take such steps as the Commission considers necessary for those purposes.

50. Enforcement notices are provided by section 133 of the Act:

(1) In this Part, “enforcement notice” means a notice in writing served in accordance with subsection (2), subsection (3) or section 109(5)(d), 115(2), 122(4)(d) or 127(2), on a controller or processor, requiring the controller or processor to take such steps as are specified in the notice, within such time as may be so specified...

51. It seems that no enforcement notice was issued by the DPC following the Inquiry. The Decision would appear to meet the requirements of an enforcement notice within the meaning of section 115(2), a notice in writing requiring the taking of one of the corrective measures set out in Article 58(2) of the GDPR. However, at the hearing of the appeal, the court was advised by the DPC that it did not consider that the Decision should be treated as an enforcement notice, the DPC apparently being of the view that an enforcement notice would only issue if a requirement imposed by a decision was “*not obeyed*” (Transcript, Day 9, p 140, lines 3 -5). That does not appear to accord with the scheme of the 2018 Act, but no issue was taken by TikTok with the absence of an enforcement notice, so I do not need to consider this issue further.

52. The relevant provisions of section 142 provide as follows:

(1) Without prejudice to section 150, a controller or processor that is the subject of a decision under section 111, 112, 113 or 133(9) to impose an administrative fine may, within 28 days from the date on which notice of the decision concerned was given to it under section 116 or, as the case may be, section 133(9)(b) appeal to the court against the decision.

(2) The court, on hearing an appeal under subsection (1), may consider any evidence adduced or argument made by the controller or processor concerned, whether or not already adduced or made to an authorised officer or the Commission.

(3) Subject to subsections (4) and (5), the court may, on the hearing of an appeal under subsection (1)—

(a) confirm the decision the subject of the appeal,

(b) replace the decision with such other decision as the court considers just and appropriate, including a decision to impose a different fine or no fine, or

(c) annul the decision ...

53. Finally, section 150 is in the following terms:

(1) A controller or processor on which an information notice or enforcement notice or a notice under section 135(1) is served may, within 28 days from the date on which the notice is served, appeal against a requirement specified in the notice.

(2) The court, on hearing an appeal under subsection (1), shall—

(a) annul the requirement concerned,

(b) substitute a different requirement for the requirement concerned, or

(c) dismiss the appeal.

(3) This subsection applies to an appeal brought under subsection (1)—

(a) against a requirement specified in an information notice to which section 132(3) applies, or an enforcement notice to which section 133(6) applies, and

(b) that is brought within the period specified in the notice concerned ...

The Inquiry

54. In the Decision, the DPC describes the TikTok platform as follows:

“36. The TikTok platform is a social media service allowing users to create and share short-form videos of up to 10 minutes in length. It is available as an app for Android and iOS, and via the website www.tiktok.com. TikTok accounts can be created by users aged 13 years and over using a phone number and email address. A TikTok profile typically contains a profile photo or video and username. The app shows a personalised ‘For You’ feed of videos for each user, recommended based on factors such as the user’s selected interest categories, device and account settings, and interaction with the app. Users can create, watch, ‘like’ and comment on videos, ‘follow’ other users’ profiles, and send direct messages to other users.

37. The TikTok platform is understood to have more than 1 billion monthly active users globally as of 27 September 2021. TikTok Ireland has informed the DPC that in May 2022, the TikTok platform had approximately 128 million monthly active users in the EEA. TikTok also reports, pursuant to its obligation under Article 24(2) of the Digital

Services Act, that it had on average 159 million monthly active recipients in the European Union member state countries between July 2024 and December 2024.

38. *TikTok Ireland has stated that the TikTok service is not offered or available in China, where the ByteDance group of companies separately operates “a similar but entirely distinct” video-sharing platform called Douyin...”*

55. ByteDance Limited (“**ByteDance**”) is TikTok’s ultimate parent. Though it is registered in the Cayman Islands, many of the ByteDance group of companies and its employees are based in China.

56. For the purpose of these proceedings, it is not in dispute that TikTok acts as a controller, within the meaning of Article 4(7) of the GDPR in respect of the personal data on the TikTok platform, that it has its main establishment in Ireland, that it engages in the cross-border processing of data and that the DPC is the competent authority to act as LSA for the cross-border processing of data the subject of the Inquiry in accordance with the procedure set down in Article 60 of the GDPR.

57. As appears from the Decision, during the course of its supervision interactions with TikTok, the DPC was informed by TikTok that certain personnel located in China accessed personal data of TikTok’s EEA users in order to provide support services in connection with the operation of its platform, including functions related to software engineering, maintenance and development. On 26 March 2021, TikTok provided the DPC with its data transfer assessment (“**DTA**”) for China, an assessment of the level of protection afforded to data transferred to China, together with supporting documentation. This DTA identified that there was a divergence between the level of protection afforded to personal data in China from that afforded within the EU, but concluded that, in light of standard contractual clauses together with supplementary measures employed by TikTok, personal data transferred to China was afforded essentially equivalent levels of protection to that guaranteed within the EU. The DTA was updated four times throughout the Inquiry. Each DTA reached the same overall conclusion. The five DTAs are addressed together in the next section of this judgment.

58. On 7 April 2021, the DPC received a submission from Stichting Onderzoek Marktinformatie, a Dutch non-governmental organisation, raising concerns about the processing of personal data by TikTok, due to risks for young users, and the non-EEA transfer of personal data.

59. On 28 May 2021 and 5 July 2021, the DPC received requests for mutual assistance from the French supervisory authority, Commission Nationale de l'Informatique et des Libertés, requesting that the DPC investigate matters pertaining to TikTok's transfer of personal data to China.

60. On 14 September 2021, the DPC notified TikTok of the commencement of two inquiries pursuant to section 110 of the Data Protection Act 2018 (so-called "own volition" inquiries), including the inquiry which led to the decision the subject of these proceedings ("**the Notice of Commencement**" or "**the Notice**").

61. The Notice of Commencement explained the background to the Inquiry and the legal basis for it. It identified that the Inquiry would focus on three specific issues as follows:

Issue 1:

With regard to TikTok's analysis of China's laws and practices that impact data protection of EEA users, what specific issues did it identify that indicated that Chinese laws and practices do not provide protection essentially equivalent to that in the EU and that would require TikTok to implement supplementary measures?

Issue 2:

Concerning GDPR Chapter V whether TikTok can demonstrate it has fulfilled its Chapter V obligations with regard to transfers of personal data in terms of the effectiveness and/or appropriateness of the supplementary measures applied to personal data transfers to China. Can TikTok demonstrate how the supplementary measures specifically overcome the deficits in protection identified in terms of the laws and practices of China to provide a level of protection essentially equivalent to the one guaranteed in the EEA?

Issue 3:

Concerning GDPR Article 13(1)(f) whether TikTok can demonstrate that it has fulfilled its obligations with regard to provision of information to its users in relation to transfers of personal data to China.

62. The notice also set out the procedure which would be followed by the DPC in the Inquiry, highlighting the fact that it would be subject to the provisions of Article 60 of the GDPR. It noted that following its information gathering it would prepare a “*Draft Decision*” for the purpose of the Article 60 process. The notice stated that the “*Draft Decision will be furnished to TikTok for its consideration and submissions before it is submitted to the Article 60 process.*” As appears from the following, the DPC did not, in fact, adopt the precise procedure mapped out in the Notice.

63. Attached as an appendix to the Notice of Commencement was a request for information (“**the first RFI**”) containing five questions regarding the “*data transfers*”.

64. TikTok responded to the Notice of Commencement and the first RFI on 12 October 2021. The response included an updated DTA. A further updated DTA was provided on 28 January 2022. Each reached similar conclusions in relation to the personal data being transferred to China.

65. On 11 May 2022, the DPC requested further information from TikTok (“**the second RFI**”). This request was far more detailed than the first RFI and raised queries under the headings ‘*General*’, ‘*Remote Access by the China Group Entities*’, ‘*Intra-Group Agreement and the 2010 SCCs*’, ‘*Article 49 Derogations*’, and ‘*Analysis of Chinese Legal Framework in the Data Transfer Assessment*’.

66. The first question posed under the ‘*Remote Access*’ heading was the following:

Please further clarify the circumstances and in particular the technical means by which personal data is remotely accessed by personnel of the China Group Entities, referring to or further clarifying the information set in the Data Transfer Assessment and TikTok Ireland’s Response dated 12 October 2021 (in particular pages 16 to 17, paragraphs 12.8 to 12.9 of same, as appropriate).

67. Under the last heading, ‘*Analysis of Chinese legal framework in the Data Transfer Assessment*’, the DPC raised the following query (Query V(3)) :

Please further clarify the factual and legal basis for TikTok Ireland’s position that problematic laws and practices in China are not at risk of being applied to the transfers the subject of the Inquiry in circumstances where the personal data of EEA users is stored outside of the territory of China, but is processed by the China Group Entities within the territory of China.

* emphasis in original

68. Having sought an extension of time to provide a response, TikTok responded on 20 June 2022 on a query-by-query basis to the questions raised. Its response to the query about the technical means by which personal data is remotely accessed detailed the access restrictions imposed but did not explain what was actually happening when data was transferred. Its response to Query V(3) was as follows:

Chinese authorities do not have the power to compel disclosure of the remotely accessible EEA User Data, have not made any such requests and, in the extremely unlikely event that such request was made, the China Group Entities would be entitled to refuse it. Accordingly, the China Group Entities are in a position to comply with the 2010 SCCs. This is explained further below...

69. The response then further explained the territoriality principle on which TikTok relies.

70. On 7 July 2022, the DPC provided TikTok with a detailed Statement of Issues and invited submissions on same. The issues for determination were summarised as follows:

(1) The DPC will consider and determine, within the scope of the Inquiry, the relevant facts as to TikTok Ireland’s reliance on the 2010 SCCs in connection with the transfers the subject of the Inquiry involving remote access to personal data of EEA users by the China Group Entities.

(2) The DPC will consider and determine, within the scope of the Inquiry, the relevant facts as to the scope of TikTok Ireland’s reliance, if any, on the derogations set out in

Article 49 GDPR, and in particular Article 49(1)(b) GDPR, and, if necessary, review and determine the lawfulness of same in the context of the transfers the subject of the Inquiry.

(3) The DPC will consider and determine within the scope of the Inquiry whether TikTok Ireland can demonstrate that it has complied with its responsibility to assess the level of protection of personal data of EEA users the subject of transfers to the China Group Entities using SCCs under Article 46(2)(c) GDPR for the purpose of Articles 44 and 46(1) GDPR, having regard in particular to TikTok Ireland's responsibility as a controller in light of Article 5(2) and 24 GDPR. This will include consideration as to whether TikTok Ireland has adequately assessed whether, and the extent to which, there is a risk that the personal data of EEA users remotely accessed by the China Group Entities may be subject to potentially problematic laws and practices in effect in China, and whether, and extent to which, there is a risk that the 2010 SCCs are not being complied with, or cannot be complied with, by the China Group Entities in the context of the transfers the subject of the Inquiry.

(4) The DPC will consider and determine, within the scope of in the Inquiry, whether TikTok Ireland can demonstrate that the supplementary measures implemented by TikTok Ireland and the China Group Entities in respect of the remote access by the China Group Entities to personal data of EEA users are effective, together with the 2010 SCCs, to ensure that EEA users are provided with the appropriate safeguards, enforceable rights and effective legal remedies required by Articles 44, 46(1) and 46(2)(c) GDPR, so that the personal data of EEA users is afforded a level of protection essentially equivalent to that guaranteed within EU by the GDPR.

(5) The DPC will consider and determine whether TikTok Ireland has complied with its obligations under Article 13(1)(f) GDPR with reference to the information it provides to EEA users of the TikTok platform concerning the transfers the subject of the Inquiry.

71. When furnishing the Statement of Issues, the DPC indicated that in respect of the second issue, it intended having regard to information on government access to personal data in China set out in the “*Final Report EDPS/2019/02-13, Legal study on Government access to data in third countries for the EDPB (November 2021)*” (“**the Milieu Report**”).

It seems clear that the question of public authority access to data transferred by TikTok to China was becoming the focus of the Inquiry.

72. TikTok raised certain queries on the Statement of Issues and responded in substance on 15 September 2022. TikTok notified the DPC of its intention to submit expert evidence in relation to the Milieu Report. It also informed DPC that it was in the process of updating its DTA for China and expected to complete this by 13 October 2022. It also stated that it was in the process of updating its EEA privacy policy, and that it would shortly be amending its Intra-Group Agreement for the purpose of transitioning from the 2010 standard contractual clauses (“**the 2010 SCCs**”) to the new SCCs (“**the 2021 SCCs**”), and that this would be done by 27 December 2022. TikTok also queried the temporal scope of the Inquiry and were advised it was “*ongoing*”. The substantive response identified a number of “*procedural issues*”, including querying whether the DPC was involved in further fact finding. In a response dated 3 October 2022, the DPC appeared to indicate, by reference to an earlier letter dated 25 July 2022, that fact-finding was not complete.

73. On 13 October 2022, TikTok provided the DPC with an expert opinion on Chinese law, addressing the Milieu Report, from Professor Ke Xu, Associate Professor of Law of the Law School, University of International Business and Economics, Beijing (“**the first Xu opinion**”). It also provided an update to the DTA (“**the October 2022 DTA**”). It provided its updated privacy policy on 22 October 2022, and information on the 2021 SCCs in December 2022.

74. The DPC sent a request for further information on 21 February 2023, raising queries regarding the 2021 SCCs (“**the third RFI**”).

75. When responding to this request on 28 March 2023, TikTok provided information on further measures it was putting in place, referred to as Project Clover, to ensure the protection of EEA user data. It advised that the measures comprising Project Clover were at an advanced stage of design and implementation had already commenced. No clear evidence of implementation of any particular measure within the temporal scope has ever been provided by TikTok and in the circumstances, I have treated the Project Clover measures as having been implemented outside the temporal scope of the Inquiry.

76. The DPC raised queries about the turnover of TikTok's parent company, ByteDance, in April 2023. On 17 May 2023, it issued a Preliminary Draft Decision ("**the PDD**"). The PDD defined the temporal scope of the Inquiry as commencing on 29 July 2020 and ongoing.

77. In relation to Issue 1 (of the Statement of Issues), the PDD identified the following facts which it proposed to have regard to as established for the purpose of the Inquiry (at §165):

165.1. I am satisfied that the remote access by personnel of the China Group entities to personal data of EEA users of the TikTok platform stored on servers in Singapore and the Unities States is a "transfer" of personal data for the purposes of Chapter V of the GDPR. This not disputed and is supported by the Supplementary Measures Recommendations.

165.2. I note, in that regard, that the position under the 2010 SCCs was, and under the 2021 SCCs remains, that EEA user data is stored on servers located in Singapore and the US, and is not itself stored on servers in China.

165.3. I am also satisfied that from 29 July 2020 to 19 December 2022, the transfers were made pursuant to the 2020 Intragroup Agreement implementing the 2010 SCCs, and from 19 December 2022 to date, the transfers were made pursuant to the 2022 Intragroup Agreement implementing the 2021 SCCs.

165.4. The situation under the 2010 SCCs was that transfers were made directly by TikTok Ireland as controller to 26 China Group Entities acting as processors until 13 October 2022, and to 16 China Group Entities acting as processors thereafter. Under the 2021 SCCs, the transfers are made directly, in the first instance, to one of the China Group Entities acting as processor, and then onward to one or more of the 15 other China Group Entities acting as subprocessors. The processing may engage one or more of multiple processors located in China.

165.5. I have had regard to the circumstances of the remote access as outlined by TikTok Ireland under both the 2010 SCCs and the 2021 SCCs. Both the factual description of the remote access, and the information furnished in respect of the nature of the processing lead me to believe that the transfers are regular, systematic, and frequent.

The transfers are made for a large and complex range of tasks and functions performed by the China Group Entities that appear essential to the operation of the TikTok platform. When remote access is authorised for a specific business purpose, it is in general authorised for up to 12 months, a considerable length of time.

165.6. The purposes for which the transfers were made under the 2010 SCCs, and the 2021 SCCs are extensive, and the categories of personal data, and, indeed, the volume of personal data in terms of individual data points relating to each user that may be the subject of the processing are very significant in number. This must be viewed relative to the fact that TikTok is a popular and widely used platform with approximately 128 million users in the EEA as of May 2022.

165.7. The personal data of EEA users may be accessed remotely by the China Group Entities may include sensitive data (aligning broadly to the concept of personal data that may fall within Articles 9 and 10 of the GDPR). It may also include, based on a demonstrated business need, personal data in decrypted or plaintext form.

165.8. At present, based on TikTok Ireland's submissions, I am not led to form the view that personal data of EEA users of the TikTok platform with other ByteDance companies in China for use in other ByteDance products (such as Toutiao and Douyin).

78. The final paragraph should, it seems, include the words “*is being shared*” after the words “*users of the TikTok platform*”, i.e. the DPC formed the view that EEA user data is not shared for use in ByteDance Chinese platforms.

79. In its analysis of Issue 2, the PDD commented as follows in relation to the information provided by TikTok in relation to Chinese law (at §210):

In light of the above, I have considered the manner in which I should assess information furnished by TikTok Ireland relating to the content, meaning or effect of Chinese law in the context of this PDD. Where TikTok Ireland has confirmed that the legal analysis in Section 2 of the Data Transfer Assessments was “prepared by one of China’s leading independent law firms”, I have taken the information set out in the PDD at its height, and at face value, with regard to its veracity. However, in the context of the Inquiry, I

am obliged to ensure that I am satisfied that there is sufficient information and evidence to enable me to review and verify TikTok Ireland's assessment, and ultimately to conclude that the personal data of EEA users is afforded appropriate safeguards in the context of transfers to China the subject of the Inquiry. A failure on TikTok Ireland's part to verify, guarantee and demonstrate adequate protection would render the data transfers unlawful.

80. The PDD identified that notwithstanding TikTok's analysis of the territoriality principle, there remained "two key concerns" which were set out at §254 – §257 of the PDD. Given the centrality of these paragraphs to TikTok's appeal, it is appropriate to set these paragraphs out in full:

253. I have had due regard to the above submissions, in particular with regard to the effect of the territorial principle in Chinese law. While I note TikTok Ireland's analysis in this regard, I nonetheless remain with two key concerns.

254. The first concern takes as its premise that TikTok Ireland's analysis of the application of the territoriality principle in Chinese law in the specific factual context is fully correct. The concern relates to those laws such as the Anti Terrorism Law, Counter-Espionage Law, Cybersecurity Law or the National Intelligence Law that may be interpreted to have extra-territorial effect, to the extent that activities within their scope constitute a crime under either that legislation itself, or the Criminal Law. I note TikTok Ireland's acknowledgement that, insofar as aspects of their application are not as clear and precise as required by the EU standard, these laws would not comply with the requirements for necessity and proportionality required by EU law. As such, these laws, are, in my view, problematic, and although TikTok Ireland has submitted that this could only arise in practice in rare or exceptional cases, it does not dispute the risk that they may apply extraterritorially to enable Chinese authorities to exercise jurisdiction under Chinese law to request disclosure of personal data of EEA users the subject of the transfers and remote access by the China Group Entity. For example, Article 10 of the National Intelligence Law expressly provides for intelligence activities both within and outside of China. The second concern relates to the basis for the premise that TikTok Ireland's analysis regarding the application of the territoriality principle in the specific factual context of the transfers is accurate. The concern itself is that TikTok

Ireland has furnished insufficient information in the Inquiry to enable me to conclude that the territoriality principle does in fact operate so as to prevent the application of problematic surveillance laws, such as the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law and National Intelligence Law, to the personal data of EEA users the subject of the transfers, save in situations where those laws have extra-territorial effect. This leads to the conclusion that TikTok Ireland has itself failed to verify, guarantee and demonstrate the adequacy of the protection in respect of the Data Transfers.

255. In this regard, having reviewed the Data Transfer Assessments, I do not consider that TikTok Ireland has demonstrated the basis for its conclusion that those laws, which clearly have effect within the territory of China, could not be used to compel the China Group Entities or their employees (who are persons within the territory of China and the jurisdiction of the Chinese authorities) to provide assistance in accessing or disclosing personal data stored in the territory of foreign States but remotely accessed within the territory of China.

256. In particular, I do not agree that it has been sufficiently demonstrated how the China Group Entities, or their employees, who are personally within the jurisdiction of China and the Chinese authorities, would fall outside of the scope of laws such as the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law and National Intelligence Law which appear to provide for broadly defined obligations on persons within the jurisdiction of China to assist with the work of its surveillance authorities. In short, it is not clearly explained why it would not be open to the Chinese authorities to impose obligations on the employees of the China Group Entities, who are able to access the personal data contained on servers in the US and Singapore from China, to provide the Chinese authorities with such data.

257. I consider, further, that TikTok Ireland's submissions, and Data Transfer Assessments, are vague in describing the exact contours of the territoriality principle. Although it is described as a fundamental norm of Chinese law and various provisions of the PRC Constitution and other legal measures are referenced in support of its existence, the text of these provisions do not, in my view, sufficiently delineate the contours of this principle to enable me to be satisfied of the manner of its application

to the laws and practices outlined by TikTok Ireland in Section 2.2 of the Data Transfer Assessment. Further, I note that TikTok Ireland does not refer to legal authorities that interpret this principle in practice in a scenario that is analogous to the present one, concerning remote access, using technical means, by persons within the jurisdiction of China to data stored on servers in a foreign jurisdiction.

81. These concerns led the DPC to form the provisional view on Issue 2 that TikTok had failed to “*verify, guarantee and demonstrate*” that the level of protection was essentially equivalent to that provided by EU law (at §299.3 of the PDD).

82. These concerns also informed the DPC’s analysis of Issue 3. The DPC’s preliminary views in respect of that issue are set out at §368 - §371

368. The supplementary measures are not effective in addressing the risk that Chinese authorities could impose obligations on the employees of the China Group Entities, who are able to access the personal data contained on servers in the US and Singapore from China, to provide the Chinese authorities with such data. The system entry controls and Network Security measures, while reflective of general security, cannot act to prevent access under problematic laws. Encryption of the EEA user data in transit, along with the storage of the master keys outside of China, does not address the risk of Chinese authorities accessing the personal data that is accessed in by employees of the China Group Entities in plain text. TikTok Ireland has set out a broad range of purposes for which personal data is accessed remotely in plain text. TikTok Ireland has also set out the broad nature of what this processing entails. This Preliminary Draft Decision sets out how these transfers in plain text are systematic, repetitive, and continuous. Therefore, I consider that the encryption measures implemented do not compensate for the lack of essentially equivalent protection outlined above in light of the data that is accessed in plain text. While the physical separation is good practice in terms of a security measure, this does not address the issue of the risk of Chinese authorities imposing obligations on the employees of the China Group Entities in respect of the personal data accessed in plain text. This personal data may be subject to such access irrespective of whether it was originally encrypted at rest. Furthermore, in any event, the Master keys being stored outside of China, naturally, does not prevent remote access to them from China.

369. *The contractual measures are merely contractual in nature and are not binding on public authorities in China. Furthermore, in respect of the contractual provisions regarding the obligation to notify TikTok Ireland, while TikTok Ireland has outlined the situations in which the public authorities of China may impose confidentiality obligations or may request a disclosure request be kept confidential by the person or entity that is the recipient of the request, it has failed to assess how these aspects of Chinese law affect the suitability of the contractual measures as supplementary measures in terms of compensating for the lack of essentially equivalent protection. By failing to clarify these issues in its assessments, TikTok Ireland has failed to comply with its responsibility to adequately assess the level of protection of EEA users under the Chinese legal framework for the purpose of Articles 44 and 46 GDPR, and, further, has failed to comply with its obligation to demonstrate its compliance with Articles 44 and 46 of the GDPR with regard to the processing the subject matter of the transfers.*

370. *The access controls, in light of the broad nature of the purposes for which the personal data is remotely accessed, and the systematic, repetitive, and continuous nature of the transfers, are of limited utility in terms of compensating for the lack of essentially equivalent protection. These access controls do not address the potential for Chinese authorities to impose obligations on the employees of the China Group Entities, who access the data for broad purposes, to provide the Chinese authorities with such data. Therefore, they so [sic] not compensate for the lack of essentially equivalent protection outlined above.*

371. *TikTok Ireland's assessments failed to verify, guarantee, and demonstrate that the supplemental measures or the SCCs address the identified risks associated with the transferred data falling the subject to laws in China, such as the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law or the National Intelligence Law. I provisionally find that TikTok Ireland has failed to verify, guarantee and demonstrate that the supplementary measures and the SCCs are effective to ensure that the personal data of EEA users is afforded a level of protection essentially equivalent to that guaranteed within the EU. Therefore, in light of the analysis above, I provisionally find that TikTok Ireland's has failed to provide appropriate safeguards in respect of the data transfers and its reliance on Article 46 GDPR for the data transfers is invalid.*

83. The DPC also made preliminary findings in relation to Article 49 of the GDPR which are not necessary to consider for the purposes of these proceedings. Taking the preliminary findings in relation to Issues 1 to 4 together, the DPC made the following “*provisional finding of infringement*” (at §398):

[T]hat TikTok Ireland had infringed Article 46(1) GDPR regarding the Data Transfers by failing to verify, guarantee and demonstrate that the supplementary measures and the SCCs are effective to ensure that the personal data of EEA user is afforded a level of protection essentially equivalent to that guaranteed within the EU”.

84. In relation to Issue 5, the question of whether TikTok had complied with its obligations under Article 13(1)(f) of the GDPR, the DPC formed the preliminary view that TikTok’s October 2021 Privacy Policy failed to comply with the requirements of Article 13(1)(f). Its updated December 2022 policy was assessed as compliant (see §432 of the PDD).

85. In light of those preliminary views and findings, the DPC provisionally decided (i) to make an order pursuant to Article 58(2)(j) requiring TikTok Ireland to suspend the Data Transfers, (ii) to make an order pursuant to Article 58(2)(d) GDPR requiring TikTok Ireland to bring the processing into compliance in the manner specified in the PDD, and (iii) to impose two administrative fines pursuant to Article 58(2)(i) GDPR in the ranges of €450 - €500 million and €30 - €50 million respectively (see §437 of the PDD).

86. TikTok made submissions on the PDD on 8 September 2023. It provided a second opinion from Professor Xu (“**the second Xu opinion**”), reports from two law firms, Fangda and Clifford Chance, a technical report on Project Clover (“**the Project Clover Technical Report**”) and a report from NCC Group regarding the Project Clover measures. The Project Clover measures are described below.

87. On 29 September 2023, TikTok provided a report from Dr Prateek Mittal concerning TikTok’s privacy solution (“**the Mittal report**”). Dr Mittal is Professor in the Department of Electrical and Computer Engineering at Princeton University. He is also an affiliated faculty at Princeton University’s Center for Information Technology Policy, Andlinger Center for Energy and the Environment, and the Department of Computer Science. His

report notes that he has published over 100 papers at peer-reviewed conferences and journals in the field of privacy and security.

88. The Mittal report concluded as follows:

By virtue of the mathematical guarantees provided by TikTok's Differential Privacy Solution, an adversary would not be able to determine with a reliable level of confidence (through any possible means either currently available or devised in the future and using any other internal or external data either currently available or obtainable in the future), any incremental information about any attribute of any single individual (or even the presence of any single individual) from Differentially Private Aggregated Data. This results in Differentially Private Aggregate Data that are effectively anonymous, in line with the GDPR, for individual personnel working for the CGEs (or their employee groups).

89. TikTok provided an updated DTA on 6 October 2023 (“**the October 2023 DTA**”).

90. In its written response to the PDD, TikTok made the following submission which now forms one of the central planks of its appeal (at §13):

For the reasons explained in Sections IV and Section VI, Part B of this Response, TikTok submits that the manner in which the issues have been drawn by the DPC does not accord with the judgment of the CJEU in Schrems II. Specifically, insofar as the DPC contends that TikTok has failed to adequately assess whether, and the extent to which, the SCCs are not being complied with and/or cannot be complied with by the China Group Entities in the context of the Data Transfers, it is incumbent on the DPC to investigate and carry out this assessment itself by reference to the relevant provisions of Chinese law and having regard to the circumstances of the Data Transfers. A suspension order can be made only if the DPC, having carried out this assessment, makes a finding that: (i) potentially problematic laws and practices in China have the effect that the China Group Entities cannot comply (or are not complying) with the SCCs, and (ii) the protection of the EEA User Data transferred that is required by EU law cannot be ensured by other means.

91. As indicated, this submission was elaborated on at sections IV and VI of the response document and was reflected to a significant degree in the submissions made in this appeal. Notwithstanding that the Notice of Commencement had requested that TikTok demonstrate to the DPC that the transferred data was afforded equivalent protection in China, this appears to have been the first occasion where TikTok suggests, in effect, that it was under no obligation to do so.

92. On 8 February 2024, the DPC wrote to TikTok seeking clarification on matters arising from TikTok's response to the PDD, including whether remote access by personnel in China involved storage of EEA user data in China, including temporary storage. The requests for clarification were not described as a request for further information, but this letter was characterised by TikTok as the fourth RFI at the hearing. Though the DPC pointed out that it was not so described, it accepted that this had no legal significance. I will, accordingly, refer to it as the fourth RFI in this judgment. The covering letter stated:

Since the commencement of this Inquiry, TikTok Ireland has been consistent in its position that EEA User data is not stored on servers in the People's Republic of China ('China'). However, as I understand it, TikTok Ireland's response to the Preliminary Draft Decision represents the first instance in which TikTok Ireland has claimed that no storage of any kind, including temporary storage, of EEA User Data occurs in China.

During the Inquiry, TikTok Ireland outlined the circumstances in which the China Group Entities obtain remote access to EEA User Data stored in the Global Data Centres. In this regard, TikTok Ireland has outlined to the Inquiry that there is remote access through applications and other measures that enable the foreign State servers to be accessed from China. For the purpose of confirming whether that remote access results in the storage of EEA User Data in China, including temporary storage, please respond to the queries set out in the Schedule to this letter...

93. The suggestion in the letter that the response to the PDD was the first time that TikTok had claimed that there was no storage of any kind, including temporary storage in China seems to have been an inference drawn by the DPC from the response. There is no reference to temporary storage in the response to the PDD, though TikTok does state that no EEA user data is stored *on servers* in China.

94. The issues raised in the schedule to the letter were as follows:

1. Please describe in detail the manner in which computer information systems and devices within the territory of China enable the China Group Entities to obtain remote access to EEA User Data. This description must outline:

(i) The technological operations deployed on those computer information systems and devices that enable personnel within the China Group Entities to interact with EEA User Data;

(ii) The technical solution used to provide such interaction, including a description of the physical location of the technical architecture (such as multi-tier, client- server models) and the interaction with any ICT security layers that protect information in transit between the servers and the presentation layers (to include the location of physical gateway devices on the transport layer and how those interact with any VPN tunnelling);

(iii) Any permanent or temporary storage of EEA User Data that occurs on computer information systems and devices including within the territory of China, including, but not limited to storage or processing by means of any Central Processing Unit, Main Memory, Random Access Memory, Secondary Storage or any other element of the computer information systems, networks, and devices located in China;

(iv) Any processing, as defined in Article 4(2) GDPR, of EEA User Data that occurs on computer information systems and devices within the territory of China;

(v) The means by which TikTok Ireland shares information with personnel within the China Group Entities, and the means by which that data and how that data is made available for those personnel; and

(vi) The applications and other measures that enable the foreign State servers to be accessed from China.

2. If it is the case that the China Group Entities obtain remote access to EEA User Data without any EEA User Data being stored temporarily or permanently on computer information systems and devices in China, please outline the technical means by which personnel within the China Group Entities can view and interact with that data without any temporary or permanent storage occurring in China.

95. At the hearing, the DPC characterised this letter as a *repeated* request for information which had been sought previously, in particular in the second RFI, but not provided. Although in its response TikTok contended that this was the first time such information was sought, in my view, the DPC’s characterisation is reasonable. The second RFI had asked for details of the technical processes involved in the remote access and this had not been provided.

96. In its response, dated 11 March 2024, TikTok confirmed that personal data was temporarily processed in China, and that this involved a transfer of data for the purpose of Chapter V of the GDPR. It suggested that this local processing was “*implicit in any remote access solution.*” The precise details of the technical measures described will be addressed below.

97. The response also stated, in apparent response to the DPC’s second query:

Second, TikTok does not consider that the use of the Remote Access Solution results in any “storage” of EEA User Data in China. In particular, TikTok does not consider that the processing carried out in China in connection with the Remote Access Solution is storage or a storage solution. This is because that processing does not, using the conventional meaning of “storage”, provide a location for data when it is not being used, so that it can be later retrieved for any purpose.

98. This passage included a footnote in which English-language dictionary definitions of the word “*storage*” were provided.

99. In the response, TikTok sought confirmation that the DPC would have regard to the materially new information provided by it since the PDD. It requested that the DPC withdraw the PDD and issue a revised PDD in light of the new measures which TikTok had put in place. In a letter dated 18 April 2024, TikTok suggested that an in-person meeting to discuss Project Clover would be the “*optimal format*” to explain its technical features and implementation and any other queries arising.

100. TikTok repeated the request for a revised PDD in letters dated 14 June 2024, 28 June 2024, 2 October 2024 and 6 December 2024, stating that fair procedures required that it be

afforded an opportunity to respond to the DPC's preliminary views of its response to the PDD before a draft decision was submitted to the Article 60 process.

101. Although the DPC confirmed, in a letter dated 21 June 2024, that it would have regard to all information provided when making its draft decision (as previously advised in its letter of 15 April 2024), it declined to withdraw the PDD, stating that it considered this to be unnecessary. The letter stated that *“during the course of the DPC’s consideration of TikTok Ireland’s latest submissions, if any issue requiring clarification or further submissions arises, the DPC will inform TikTok Ireland of same.”* Despite TikTok’s requests, there was never any in-person meeting between TikTok and representatives of the DPC regarding the issues the subject of the Inquiry.

102. On 31 July 2024, TikTok provided the DPC with a further revision to its DTA (**“the July 2024 DTA”**). This is the most up-to-date DTA so far provided by TikTok. The relevant contents of this DTA are detailed below.

103. On 6 December 2024, TikTok advised the DPC that it had updated its Intra-Group Agreement to reflect changes in the processing of data in China. On 14 February 2025, it indicated that it intended to provide updates on the further implementation of Project Clover by 10 March 2025.

104. On 21 February 2025, the DPC informed TikTok that it had finalised a draft decision (**“the Draft Decision”**) and circulated it to the SACs pursuant to Article 60 of the GDPR. As stated in the Decision (at §95):

“Given that the matters under examination in the inquiry entail cross-border processing across Europe, all other supervisory authorities were engaged as SACs for the purpose of the co-decision-making process outlined in Article 60 of the GDPR.”

105. Article 60(4) of the GDPR provides that SACs may express reasoned objections within four weeks of having been consulted. The consultation period, therefore, ran until 21 March 2025.

106. The DPC provided TikTok with a copy of the Draft Decision. The temporal scope of the Inquiry pursuant to the Draft Decision was stated to be from 29 July 2020 to 17 May 2023, which was the date of the PDD.

107. The Draft Decision contained findings on each of the five issues identified in the Statement of Issues. For present purposes, the findings in the Draft Decision are mirrored in the Decision and are set out when dealing with the Decision.

108. On 14 March 2025, TikTok requested that the DPC withdraw the Draft Decision, alleging fundamental errors of fact and breaches of fair procedures. In particular, it alleged that the DPC had erred in concluding that TikTok had not assessed the application of Chinese laws to what it called “*temporary data*”:

As the processing of the Temporary Data is, as noted by the DPC, an inevitable part of remote access, TikTok Ireland’s assessment of Chinese law and the territoriality principle necessarily considered their application to the Temporary Data. Therefore, contrary to the DPC’s assertions, TikTok Ireland’s assessment did consider that, as part of Remote Access, data is transferred to China for temporary processing.

109. The letter stated that the position had been “*put beyond doubt*” by footnote 113 of the July 2024 DTA. The letter also alleged various breaches of fair procedures and contended that there was no basis for making a suspension order when the temporal scope of the Inquiry concluded on 17 May 2023.

110. On 18 March 2025, still within the consultation period with the SACs, TikTok provided a third opinion from Professor Xu (“**the third Xu opinion**”) to address a purported gap in TikTok’s assessment of Chinese law which TikTok contended had been identified for the first time in the Draft Decision.

111. By letter dated 25 March 2025, the DPC refused the request to withdraw the Draft Decision, rejecting the claims of fundamental error and breach of fair procedures. In rejecting TikTok’s contention that the processing of data in China had been addressed all along because it was an inevitable feature of the remote access solution, the DPC stated:

TikTok Ireland's subsequent correspondence that contends that these matters were addressed all along does not retrospectively remedy this failure to verify, guarantee and demonstrate an essentially equivalent level of protection. Furthermore, even considering TikTok Ireland's most recent correspondence in the context of the ongoing transfers, it is clear that fundamental flaws identified in the Draft Decision remain unaddressed and ongoing.

112. The letter invited submissions from TikTok on the administrative fines to be imposed, making clear that the submissions “*should be limited to the determination, by the DPC, of final fining amounts from within the fining ranges set out in the Draft Decision.*”

113. On 27 March 2025, TikTok made the first of a number of requests for “*a complete copy of the DPC's file.*” By letter dated 2 April 2025, the DPC stated that it had provided TikTok with all material that it had relied on in making the Draft Decision or would rely on in making the final decision. It stated that TikTok had no entitlement to details of its engagement with the other SACs and that it had already been provided with all material to which it was entitled.

114. By letter dated 11 April 2025, TikTok made submissions on the amounts of the administrative fines to be imposed. The letter also provided updates on the Project Clover measures.

115. Although the DPC received comments on the Draft Decision from three SACs (those of France, Holland and Berlin), it received no reasoned objections. Accordingly, the DPC adopted the Decision with “*non-material*” amendments from the Draft Decision on 30 April 2025.

The Decision

116. At paragraph 378 of the Decision, the DPC observed as follows:

In practice, the Data Transfers concerned remote access to the personal data by persons within the jurisdiction of China. The Remote Access Solution resulted in EEA User Data being processed on computer information systems in China. This is an inevitable consequence of any remote access solution. This processing of personal data occurs on devices within the territory of China.

117. The Decision continues:

379. Despite the fact that TikTok's Remote Access Solution results in EEA User Data being processed in China, TikTok Ireland has not established that Chinese Authorities would require extraterritorial enforcement jurisdiction to obtain access to this data when it is processed there. TikTok Ireland's assessment of the territoriality principle focused on the personal data when that data is located in Singapore, Malaysia, and the United States. The submissions set out that Chinese authorities cannot carry out intelligence gathering or investigative activities in a foreign State, and therefore cannot compel a China Group Entity or one of their personnel in China to access and disclose the remotely accessible EEA User Data stored in the US, Singapore or Malaysia. TikTok Ireland outlined that compelling a person to disclose such data would involve compelling the relevant entity/individual in China to take steps within the territory of a foreign State in order to enable the Chinese authority to access or receive data stored on a server in the territory of that foreign State, and that this would be contrary to the territoriality principle.

380. TikTok Ireland's assessment of the territoriality principle failed to properly address the fact that the personal data routinely subject to the Remote Access Solution is processed in China, and therefore is located within China, albeit on a temporary basis. TikTok Ireland failed to establish that the territoriality principle prevents the application of problematic laws to EEA User Data when that processing occurs in China."

118. The DPC concluded, therefore, that the additional information provided by TikTok had not addressed the DPC's concerns. In relation to Issue 2 in the Statement of Issues, it found:

417. For the reasons outlined above, the DPC finds that TikTok Ireland failed to adequately assess the level of protection of personal data of EEA users the subject of transfers by means of the Remote Access Solution to the China Group Entities using SCCs. While TikTok Ireland acknowledged relevant divergences between the level of protection afforded by the law and practices of China compared with European Union law, its assessment of the territoriality principle resulted in it concluding that the Data Transfers fell outside the territorial scope of the problematic laws. However, the DPC finds that TikTok Ireland's assessment of the territoriality principle failed to clarify whether, and the extent to which, such laws may apply in the context of the Data Transfers, and failed to set out in a clear way the deficiencies it acknowledged to exist in the Chinese legal framework. By failing to adequately assess the law and practices in China in the context of the Data Transfers, TikTok Ireland failed to comply with its responsibility to assess the level of protection of personal data of EEA users the subject of transfers to the China Group Entities using SCCs.

418. The DPC also finds that TikTok Ireland's failure to adequately assess the level of protection provided by Chinese law and practices resulted in it failing to verify, guarantee and demonstrate that the personal data of EEA Users subject to the Data Transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union. Under Issue 3 below, the DPC has set out how the supplementary measures were not effective to ensure that EEA Users were provided a level of protection essentially equivalent to that guaranteed in the EU in circumstances where those measures were not sufficient to compensate for the risk of problematic access by Chinese authorities supported by problematic laws. However, irrespective of that finding, for the reasons that follow, TikTok Ireland's failure in the first instance to adequately assess the level of protection of personal data of EEA Users the subject of transfers to the China Group Entities using SCCs has equally resulted in it failing to verify, guarantee and demonstrate that the personal data of EEA Users subject to the Data Transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union.

119. In relation to Issue 3, the Decision concluded:

500. *The supplementary measures were not sufficient to prevent the risk of potential application of problematic access by Chinese authorities supported by problematic laws, and, thus, were not sufficient to ensure that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within the EU. TikTok Ireland's assessment of law and practices in China and the supplementary measures implemented based on that assessment have failed to appropriately account for the risk of access supported by problematic laws to EEA User Data that is processed in China. For the reasons set out above, the DPC finds that the supplementary measures implemented by TikTok Ireland were inadequate to compensate in respect of this risk. Therefore, the DPC finds that TikTok Ireland failed to verify that EEA User Data subject to the Data Transfers would be afforded a level of protection essentially equivalent to that guaranteed within the European Union in circumstances where TikTok Ireland failed to verify that problematic laws could not be applied to EEA User Data processed in China. The DPC also finds that TikTok Ireland failed to implement appropriate safeguards and supplemental measures to guarantee that EEA User Data subject to the Data Transfers would be afforded a level of protection essentially equivalent to that guaranteed within the European Union.*

501. *Accordingly, the DPC finds that TikTok Ireland failed to verify, guarantee and demonstrate that the supplementary measures implemented by TikTok Ireland and the China Group Entities in respect of the Data Transfers were effective, together with the 2010 SCCs and the 2021 SCCs, to ensure that EEA users were provided with the appropriate safeguards, enforceable rights and effective legal remedies required by Articles 44, 46(1) and 46(2)I GDPR, so that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within EU by the GDPR.*

120. The DPC made the following finding of infringement:

569. *In light of the foregoing, as set out in Issues 1 – 4, the DPC finds that TikTok Ireland infringed Article 46(1) GDPR regarding the Data Transfers. As set out above, TikTok Ireland failed to adequately assess the level of protection provided by Chinese law and practices to the personal data of EEA Users the subject of transfers to the China Group Entities using SCCs. It failed to verify, guarantee and demonstrate that*

the supplementary measures and the SCCs were effective to ensure that the personal data of EEA Users is afforded a level of protection essentially equivalent to that guaranteed within the EU. TikTok Ireland did not, and could not, rely on the derogations under Article 49 GDPR in respect of the Data Transfers made during the temporal scope. Consequently, TikTok Ireland transferred EEA User Data to China without complying with the conditions laid down by Chapter V of the GDPR and did not identify a valid lawful basis for the Data Transfers.

570. Accordingly, during the temporal scope of the Inquiry, from 29 July 2020 to 17 May 2023, TikTok Ireland infringed Article 46(1) GDPR by carrying out the Data Transfers while failing to verify, guarantee and demonstrate that the personal data of EEA Users subject to the Data Transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union.

121. Having regard to the fact that the DPC had decided that the temporal scope of the Inquiry ended on the date the PDD was provided to TikTok, the DPC separately considered the changes made by TikTok since that date when considering whether to make any suspension or correction order.

122. The Decision records that:

691. The DPC has carefully considered all of the additional supplementary measures implemented by TikTok Ireland after the temporal scope of the Inquiry, including TikTok Ireland's latest update on Project clover provided to the DPC on 11 April 2025. The additional supplementary measures do not address the risk of Chinese authorities accessing the personal data that is accessed by employees of the China Group Entities in plain text. The DPC finds that TikTok Ireland has not demonstrated that EEA User Data subject to the Data Transfers cannot be subject to problematic access by Chinese public authorities. The DPC has also considered additional information submitted by TikTok Ireland following the Draft Decision, including the Third Xi Report. However, fundamental flaws in TikTok Ireland's assessment, as identified above, remain unaddressed and are ongoing. TikTok Ireland's ongoing failure to adequately assess the level of protection provided by Chinese law and practices to the personal data of EEA users the subject of transfers interferes with its ability on an ongoing basis to select

appropriate safeguards and supplementary measures, and prevents it from demonstrating an essentially equivalent level of protection. Therefore, the DPC's concerns regarding the Data Transfers, as set out at Issues 2 and 3 of this Decision, remain in respect of the ongoing Data Transfers. For that reason, the DPC finds that TikTok Ireland has failed on a continuing basis to demonstrate that the supplementary measures that it has implemented and the SCCs are effective to ensure that the personal data of EEA users is afforded a level of protection essentially equivalent to that guaranteed within the EU.

...

702. In light of the foregoing, the DPC orders TikTok Ireland pursuant to Article 58(2)(j) GDPR to suspend the Data Transfers in accordance with the timeline outlined below.

* emphasis added

123. The highlighted reference in §691 to the third Xu opinion necessarily represents an amendment from the Draft Decision.

124. The DPC made the following finding of infringement in respect of Article 13(1)(f) of the GDPR (at §607):

The DPC finds that TikTok Ireland infringed Article 13(1)(f) GDPR by failing, in the October 2021 EEA Privacy Policy, to provide information to EEA Users identifying the third countries to which it transferred personal data. The DPC finds that TikTok Ireland also infringed Article 13(1)(f) GDPR by failing to provide a basic factual description of the transfers involving remote access to personal data of EEA users by personnel located in China.

125. The DPC imposed administrative fines of €485 million for the infringement of Article 46(1) and €45 million for the infringement of Article 13(1)(f).

126. On 7 May 2025, TikTok wrote to the DPC noting that it “*would welcome the opportunity to engage with the DPC so that TikTok Ireland can understand and address, as expeditiously*

as possible, the DPC's concerns and therefore avoid the Suspension Order taking effect.” It suggested that it might update its DTA, “elaborating further on our analysis of how Chinese law applies to Temporary Data.” It asked that:

DPC could respond by return (and no later than Monday 12 May) to provide us with an indication of: (1) the steps that we can take to address the DPC's concerns so as to avoid the coming into effect of the Suspension Order; and (2) whether the DPC would be open to a meeting with TikTok Ireland in the week commencing 19 May 2025 to discuss the steps the DPC considers TikTok Ireland would need to take.

127. It followed up with this request on 19 May 2025. The DPC replied by letter dated 23 May 2025. It stated that it did not:

... intend to direct TikTok Ireland as to the particular steps to be taken by TikTok in order to achieve compliance with its obligations as they arise under Chapter V of the GDPR, and otherwise. In that regard, it is a matter for TikTok Ireland to identify (and implement) any and all such measures as may be necessary to achieve such compliance. If and when it does so, same will be carefully considered by the DPC in accordance with the procedure laid down in Section O of the Decision, and by reference to applicable provisions of the GDPR.

128. No updated DTA has been submitted by TikTok since the date of the Decision.

129. TikTok appealed the Decision by originating notice of motion on 27 May 2025.

The Data Transfer Assessments

130. The DTA in place at the outset of the Inquiry was dated 26 March 2021. It was updated four times, the last occasion being July 2024. All of the DTAs reached the same conclusion, in effect, that having regard to standard contractual clauses and TikTok's supplementary measures, EEA user data processed by TikTok in China was subject to an equivalent level of protection to that guaranteed within the EU.

131. Each DTA contains a section headed ‘*Regulation of Public Authority Access to Private Data*’ which, as noted above, became the focus of the Inquiry. TikTok’s assessment in the March 2021 DTA was that the level of protection involved some safeguards but was “*materially below EU standards*”. It reached the same conclusion under the headings ‘*Regulation of Data Privacy*’ and ‘*International Treaties*’. In respect of ‘*Regulatory Supervision*’, it was concluded that there was a high level of safeguards, but below EU standards. It reached a similar conclusion with regards to ‘*Rights to Redress*’.

132. The March 2021 DTA then set out the supplementary measures which TikTok had put in place in order to ensure an equivalent level of protection notwithstanding the divergence between Chinese and EU law. These were divided into technical, contractual and organisational. The executive summary to the March 2021 DTA concluded as follows:

In the specific context of Authorised Access, and in light of the assessment of China’s legal framework, TikTok accepts that SCCs alone cannot provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law. For this reason, TikTok has adopted a range of additional and complementary safeguards to supplement the effectiveness of the SCCs (i.e. through the Supplementary Measures, as summarised immediately above and described in detail in Section 3 of the Assessment). In particular, the adoption of robust technical measures, a range of binding contractual commitments that far exceed the requirements of SCCs, and sophisticated internal organisational and policy controls, together ensure that any perceived risks to EEA User Data under the China’s legal framework are minimised to the extent that they do not undermine the effectiveness of the SCCs as a transfer mechanism. Furthermore, the effectiveness of these measures is enhanced by the fact that the relevant EEA User Data is stored on servers in Singapore and the US, which means such data is stored outside the legal jurisdiction of Chinese law enforcement and government authorities. This is further supplemented by the fact that encryption master keys are stored and controlled from outside China, and likewise outside China’s legal jurisdiction. In conclusion, taking account of the relevant aspects of China’s legal framework, the SCCs together with the various Supplementary Measures ensure that EEA User Data is afforded a level of protection essentially equivalent to that guaranteed within the European Union.

133. The DTA was updated in October 2021. It noted changes in Chinese law, including the coming into force of the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), both of which were in draft form at the time of the March 2021 DTA. These laws increased the protections available for personal data in China. Nonetheless, the October 2021 DTA reached the same conclusion regarding the regulation of public authority access to private data, *i.e.* that it was below EU standards. But in light of the measures adopted by TikTok, the overall conclusion of this DTA was in the same terms as the earlier DTA.

134. The next update to the DTA, in October 2022 was, for the purpose of these proceedings, in similar terms to the earlier two assessments. The overall conclusion was in similar terms, but included the following:

These measures ensure that the China Group Entities are legally entitled, and contractually required, to reject requests from Chinese authorities in respect of the EEA User Data which they can remotely access.

In conclusion, taking account of the relevant aspects of China's current legal framework in the specific context of the secure remote Authorised Access, the SCCs together with the various Supplementary Measures ensure that EEA User Data is afforded a level of protection essentially equivalent to that guaranteed within the European Union. There is no impediment as a matter of Chinese law to the China Group Entities complying with their obligations under the SCCs in the specific circumstances of the transfers.

TikTok is provided with monthly reports which confirm over a sustained period that the China Group Entities have not to date received any requests from a Chinese authority (whether law enforcement authorities, governmental authorities or judicial bodies), whilst TikTok has similarly never received any such requests.

135. In 2021, the European Commission introduced new standard contractual clauses, the 2021 SCCs, and TikTok transitioned to these in 2022. It supplied a further revised DTA in December 2022 reflecting this transition. The conclusion in the DTA remained substantially the same.

136. TikTok supplied a revised DTA in October 2023. Though the overall conclusion was similar to the earlier DTAs, that the SCCs together with supplementary measures ensured an equivalent level of protection, the October 2023 DTA differs significantly in form from the earlier DTAs. In particular, it emphasises the reliance by TikTok on the remote access solution and analyses its significance in detail. The October 2023 DTA explains as follows:

- *The following laws provide Chinese authorities with the power to obtain access to personal data: the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law, National Intelligence Law, Criminal Procedure Law and Criminal Law.*
- *These laws have been assessed in Section 2.2 of the Data Transfer Assessment (Detailed) at Annex 2, for the purpose of determining whether the transfers might fall within their scope. The assessment shows that these laws:*
 - *do enable Chinese to obtain access to transferred data in the case of direct transmission to servers in China; and*
 - *do not enable Chinese Authorities to compel disclosure of transferred data in the case of remote access transfers.*
- *These laws do not enable Chinese Authorities to compel disclosure of transferred data in the case of remote access transfers to data stored outside China because (see Section 2.B(3) of the Data Transfer Assessment (Detailed)):*
 - *Chinese law requires mutual respect for sovereignty and territorial integrity.*
 - *Chinese law recognises that data stored outside China is subject to the sovereign jurisdiction of the relevant foreign State, even if it can be remotely accessed from China. Chinese law focuses on where the data is stored, not the location of the person to whom the request is made.*
 - *Chinese authorities must have both extra-territorial “adjudicative jurisdiction” and “enforcement jurisdiction” to compel disclosure of data stored in a foreign State:*
 - o *“Adjudicative jurisdiction” is the power to subject persons, things, and conduct to judicial process, and*

o “Enforcement jurisdiction” refers to the power to compel compliance in accordance with the law.

- It is unlikely that a Chinese authority would have adjudicative jurisdiction under the above laws in respect of acts occurring outside of China (e.g. where a non-Chinese citizen commits a crime or engages in terrorist activities against China or citizens of China), but it is possible in limited cases. However, even then, no Chinese laws give Chinese authorities enforcement jurisdiction to obtain (directly or by compelling an entity or person to disclose it) data stored in a foreign State.

- If Chinese authorities want to access data stored outside of China, they must go through a mutual legal assistance or other diplomatic process.

- TikTok’s transfers to the China Group Entities are made by way of remote access to EEA User Data stored on servers in the US, Malaysia, and Singapore (not China). The assessment thus shows that Chinese authorities cannot compel disclosure of the transferred EEA User Data.

137. This summary of TikTok’s position is elaborated on in detail under the heading ‘Regulation of Public Authority Access to Private Data’. Under a heading to the effect that Chinese law is territorial in nature and does not have extra-territorial effect unless expressly provided for in Chinese law, the October 2023 DTA contained the following statement:

The Chinese laws discussed in this Section 2.2B with extraterritorial adjudicatory jurisdiction do not grant extraterritorial enforcement jurisdiction that would enable Chinese authorities to compel a person or individual in China to disclose data stored in a foreign State. This is consistent with the extension of the traditional territorial principle to cyberspace and the “respect for sovereignty and territorial integrity” principle under the Chinese Constitution, Foreign Relations Law and other laws.

138. The final DTA submitted by TikTok during the Inquiry was the July 2024 DTA. The covering letter with this DTA said it included the following material updates:

- New technical measures
- Recent changes to Chinese law since the last DTA

- Continued confirmation that TikTok has not received any requests from Chinese authorities for access to EEA User Data
- Updated factual information regarding government access to data held by third parties
- Re-organising the presentation of the summary of the Chinese National Security Law

139. The letter stated that:

Given the importance the DPC attached in its Preliminary Draft Decision to the previous data transfer assessments, we anticipate you will want to consider these latest updates carefully as part of the ongoing Inquiry.

140. The July 2024 DTA contained a similar section on regulation of public authority access to private data to the preceding DTA. In particular, it included precisely the same paragraph as that quoted from the December 2023 DTA immediately above. However, the paragraph concluded with the following footnote in the July 2024 DTA, footnote 113, upon which TikTok placed significant reliance in the appeal:

We have been advised by Fangda and Professor Xu that the transient processing inherent to the facilitation of remote access in China does not alter the above analysis. This is because the relevant data is still stored outside of China (and only remotely accessible from within China) and so is still subject to the requirements set out above. In addition: (i) such transient processing is strictly protected by the constitutional right to confidentiality of correspondence under Article 40 of the PRC Constitution and (ii) such transiently processed data would in any event still be considered offshore data when considering the scope of Chinese authorities jurisdiction (for example as a result of the logic used in Article 4 of Provisions on Data Transfer, released on 22 March 2024).

141. The July 2024 DTA also described the supplementary measures, including the additional Project Clover measures. The overall conclusion of this DTA was to similar effect to all the previous DTAs.

Scope of the appeal

142. The parties set out their positions in their initial written submissions regarding the standard of review in the appeal. However, in light of the pending judgment in *LinkedIn v DPC* the parties did not engage in detail on the issue at the hearing and sought an opportunity to make further submissions when the judgment was delivered. There are two related issues in dispute.

143. First, TikTok contended that its entire appeal is an appeal pursuant to section 142 of the Act. The DPC contends that section 142 only applies in relation to the appeal against the administrative fines, and that section 150 applies to the balance of the appeal. In *LinkedIn*, the court found that an appeal under section 142 is confined to an appeal against an administrative fine (see §138). However, in light of the court's conclusion that the same standard of review applies in relation to an appeal under section 142 and an appeal under section 150, nothing turns on this issue for the purpose of this appeal.

144. Second, TikTok contended irrespective of whether the appeal is an appeal pursuant to section 142 or 150, that it is an “*appeal on the record*” (see *Fitzgibbon v Law Society* [2015] 1 IR 516) and, therefore, the court has full jurisdiction to examine all questions of fact and law and is not obliged to defer to the DPC's decision. It also contended that it was entitled to adduce new evidence in respect of the entirety of its appeal, though it did not seek to do so. It contends that this interpretation is consistent with Article 6(1) of the ECHR, Article 47 of the Charter and Article 78 of the GDPR.

145. The DPC argued that the entire appeal is an appeal against error, citing *Orange Communications Ltd v The Director of Telecommunications Regulation* [2000] 4 IR 159 to the effect that the appellant must establish “*taking the adjudicative process as a whole, the decision reached was vitiated by a serious and significant error*”. The DPC contends that this is consistent with the CJEU's decision in Case C-26/22, *SCHUFA*, a case concerning the scope of the judicial remedy required by the GDPR.

146. Judgment in the *LinkedIn* case was delivered on 20 April 2026.

147.As appears from the detailed judgment in that case, the court (Cahill J) was asked to consider four preliminary issues in an appeal by LinkedIn from a decision of the DPC. Following a careful and comprehensive review of the issues arising in respect of each of these questions, Cahill J summarised her conclusions in relation to each of the issues as follows (at §452):

“Issue 1: Is the Appellant entitled to appeal the decision of the Respondent dated 22 October 2024 (the "Decision") under section 142 of the Data Protection Act 2018 or are there aspects of the within appeal which can only proceed as an appeal under section 150 of the 2018 Act?

Section 142 of the 2018 Act provides solely for an appeal from a decision to impose a fine. A decision that there was an infringement or infringements of the GDPR or a decision as to the exercise of other corrective powers under the 2018 Act cannot be appealed under section 142.

Issue 2: What type of appeal does section 142 of the Data Protection Act 2018 provide for and what is the standard of review/assessment to be applied by the Court in an appeal under section 142?

The form of appeal provided for in section 142 of the 2018 Act is an appeal on the record, with the possibility of new evidence or argument being admitted. Deference may be appropriate in respect of issues which are within the sphere of the DPC's technical expertise.

Issue 3: If there are aspects of the Appellant's appeal which can only proceed as an appeal under section 150 of the Data Protection Act 2018, is the standard of review/assessment to be applied by the Court the same under sections 142 and 150 of the 2018 Act or does a different standard of review/assessment apply in an appeal under section 150 of the 2018 Act?

The answer to Issue 2 applies equally to an appeal under section 150(5).

Issue 4: Having regard to the answers to the foregoing questions, is the Appellant entitled to rely on evidence adduced and/or arguments made in the Appeal which were not already adduced or made to the Respondent during the inquiry process?

It is matter within the discretion of the court to determine whether to admit new evidence or argument in an appeal under section 150(5), with the burden being possibly lighter when such an application is made in an appeal under section 142.”

* emphasis in original

148. TikTok initially indicated that it did not consider it necessary to deliver further submissions in light of the judgment, albeit it sought an entitlement to reply to any submissions which the DPC might wish to make. However, I indicated that it would be helpful for it to address the consequence for its various grounds of appeal, in particular, its fair procedures arguments, in light of the *LinkedIn* judgment and it duly delivered supplemental submissions to which the DPC replied.

149. In its supplemental submissions, TikTok highlighted the following passages from the judgment:

“Third, as LinkedIn points out, the LinkedIn Decision sets the parameters of the appeal. It seems clear that the appeal will be run on the basis of, and by way of challenge to, the LinkedIn Decision. Indeed, the right of appeal in section 142 is wholly premised on “the decision” and the orders that may be made are orders to confirm, replace or annul “the decision”. No form of appeal under that provision could be heard or determined wholly without regard to the underlying decision. A similar point was made in an authority cited by LinkedIn, Competition and Markets Authority v. Flynn Pharma [2020] 4 All E.R. 934 (“Flynn”). There the UK Court of Appeal considered the scope of the appeal from a decision of the UK Competition and Markets Authority to the Competition Appeals Tribunal. The Court noted that, while Article 6(1) ECHR was applicable,

“... the jurisdiction of the Tribunal is not unfettered. This flows primarily from the fact that the appeal is not a de novo hearing but takes the decision as its starting, middle and end point. Under s 46 CA 1998 the appeal is ‘against, or with respect to,’ the decision and includes ‘whether’ there has been an infringement. That focus upon the impugned decision is reflected in the procedural rules of the Tribunal. The appellant must identify the decision under appeal and set out why it is in error” (at [141])”

150. Since the Decision is the starting point of the Court's assessment, says TikTok, a material breach of fair procedures is capable of invalidating the decision. It notes that the DPC never contended to the contrary and refers to a letter dated 3 December 2025 from the DPC's solicitors in which it was stated that "*our client will not raise an objection to any of the grounds of appeal pleaded therein on the basis that it should properly have been pursued by way of judicial review.*"

151. TikTok refers to the decision in *Stefan v Minister for Justice* [2001] 4 IR 203 and the observation by Denham CJ (at p. 218) that:

"An applicant is entitled to a primary decision in accordance with fair procedures and an appeal from that decision. A fair appeal does not cure an unfair hearing."

152. It also refers to the observation in *Fitzgibbon v Law Society* that, in conferring a right of appeal, the Oireachtas must have intended some greater degree of review than in judicial review and refer more generally to its entitlement to an effective remedy. The submissions state as follows:

The DPC cannot be permitted to benefit from the incompleteness of a record which its own breaches of fair procedures have caused. The Court is obliged to have regard to the fact that the record could, and would, have been materially different and more comprehensive had the DPC discharged its fair procedures obligations. This is centrally relevant to the Court's assessment of whether the DPC's findings are sustainable, reasonable and rational on the evidence "on the record" and whether the conclusions drawn by the DPC can properly be upheld where TikTok was denied the opportunity to address the actual basis of the Decision.

153. It makes a further point that by reference to the refinement of the *Okunade* test in *TikTok v DPC* [2026] IESC 27 that it is "*inconceivable*" that a breach of fair procedures cannot be relied on to vitiate a decision.

154. The DPC's supplemental submissions point to cases in which the courts have concluded that defects in an earlier process can be cured by appeal.

155.Both parties made submissions regarding the degree of deference which should be afforded to the DPC's decision by reference to the particular grounds of appeal.

156.I have considerable reservations about TikTok's submission that a breach of fair procedures by a decision-maker results necessarily in the decision being invalidated in an appeal. It overlooks a number of material considerations. Its reliance on *Stefan*, and cases to similar effect is, in my view, wholly misplaced. I confess that I simply do not understand TikTok's argument by reference to the Supreme Court's refinement of the test in *Okunade*.

157.The decision in *Stefan* was a decision in judicial review proceedings challenging the decision of the respondent to refuse the applicant refugee status. The High Court granted *certiorari*, and one of the issues for the Supreme Court in the appeal was whether, in its discretion, the High Court should have refused relief on the grounds that an adequate alternative remedy was available, as it then was, an appeal to the Asylum Appeals Unit of the Department of Justice. In other words, the issue was whether, when both judicial review and an appeal are available, an applicant is *not entitled* to pursue a remedy in judicial review. The Supreme Court refused to overturn the order of *certiorari* on the grounds that, in the particular circumstance of that case, where relevant information was not before the decision maker, an appeal was not an adequate remedy.

158.*Stefan*, therefore, does not provide any support for a conclusion that where a party has available remedies by way of appeal and judicial review *and elects to pursue an appeal*, the appeal must be regarded as incapable of curing a breach of fair procedures. Indeed, *Stefan*, and the cases discussed therein, illustrate that there are many cases where an appeal will be capable of rectifying an error at first instance and is, therefore, a more appropriate form of appeal. An appeal on the record, where the court can consider the merits of the underlying decision and hear new evidence, is manifestly at least *capable* of curing a breach of fair procedures.

159.Though TikTok claim that the record is "*incomplete*", it is clear in light of the decision in *LinkedIn* (and as TikTok has always contended) that it was open to TikTok to *correct* the record, by seeking to adduce additional evidence. It did not seek to do so.

160. In addition to ignoring this obviously relevant consideration, TikTok disregards one of the key differences between the appeal provided for by the 2018 Act and judicial review. In *LinkedIn*, one of the factors relied on by the appellant and the court in concluding that the appeal provided for under section 142 and 150 was an appeal on the record was the absence of any express provision for remittal. Cahill J, correctly in my view, interpreted this as an indicator that the statutory scheme contemplated that the High Court should determine an appeal on its merits, not merely correct errors by the decision-maker.

161. If one were to take it to be the position that the court is *precluded* from remitting a decision to the DPC, then the consequence of TikTok's submission would be quite extraordinary. In judicial review proceedings, a conclusion that a decision maker had arrived at a decision in breach of fair procedures would, typically, lead to a decision being quashed and then remitted to the decision-maker for further assessment. By succeeding in the same type of argument in an appeal, on TikTok's theory, it would be left in a far better position, the decision would be annulled, but *not* returned to the decision-maker. I do not accept that an appellant can put themselves in a better position by pursuing a judicial review-type argument in an appeal on the record than had they pursued the same argument in judicial review proceedings.

162. Where an appellant *opts* to pursue an appeal where it has the entitlement to adduce new evidence and pursue new arguments, it is difficult to understand how a complaint about how the process before the decision-maker was conducted could, by itself, justify an annulment of the original decision. This is not to suggest that a breach of fair procedures at first instance is without consequence in an appeal on the record, but it cannot lead to an automatic annulment.

163. During the course of oral argument, I queried with the parties whether the court did, in fact, have an inherent or implied power to remit. TikTok's initial position was that the court could not remit an appeal to the DPC for further consideration, though it moderated that position somewhat following further engagement. Its initial position was a reflection of the statutory language of sections 142 and 150 which are framed in mandatory terms and do not reference remittal as an option available to a court.

164. TikTok accepts that there is an inherent power to remit in judicial review proceedings, which pre-dates the power contained in Order 84 of the Rules of the Superior Courts (see *Sheehan v Judge Reilly* [1993] 2 IR 81). It contended, however, that the issue had to be considered by reference to the jurisdiction conferred on the court by the 2018 Act and whether an *implied* power to remit could be found in the Act. It notes, in this regard, that there are statutory appeals to the High Court where there is an express power to remit (see, for instance, section 64 Financial Services and Pensions Ombudsman Act, 2017).

165. TikTok referred to the decision of Simons J in *O'Sheehan v Residential Tenancies Board* [2024] IEHC 521, a statutory appeal on a point of law. In that case, Simons J concluded that there was an implied power to remit, as the absence of such a power “*would undermine the effectiveness of the statutory appeal.*”

166. Reference was also made to the decision in *NzN v Minister for Justice* [2014] IEHC 31, an appeal against a revocation of a declaration of refugee status. The relevant provision of the Refugee Act 1996, section 21(5) provides that on an appeal from a decision of the Minister, the High Court may “*as it thinks proper, on the hearing of the appeal, confirm the decision of the Minister or direct the Minister to withdraw the revocation of the declaration*”. The court described the function of the court in such an appeal (at §31 and §32):

“The powers of the Court on an appeal against a revocation of refugee status is to determine whether the decision to revoke the declaration was correctly made and should be confirmed, or whether the decision was wrong and should be withdrawn. The Court can consider all the evidence which was before the Minister and hear oral evidence from the appellant and any witnesses called by either party in determining the appeal. The Court can come to its own view as to whether the decision to revoke is appropriate or should be withdrawn...”

... The Court is not empowered to ask the Minister to re-consider the decision and the Court must come to its own decision confirming the Minister's original decision to revoke the appellant's refugee status or restoring the appellant's status by directing the Minister to withdraw the revocation of the declaration. The Court does this on the

evidence which was before the Minister and any additional evidence presented on the appeal.”

167.In its oral submissions, the DPC highlighted a number of statutory appeals in which a court had remitted decisions to the decision-maker absent an express statutory power to remit, including a decision under the precursor to the 2018 Act, the Data Protection Act 1992, *Director of Corporate Enforcement v Data Protection Commission*, unreported, Circuit Court, 1 April 2022. Cases referenced included *Minister for Communications v The Information Commissioner* [2022] 1 IR 1 and *Minch v Commissioner for Environmental Information* [2017] IECA 223. It does not appear that any of those remittal decisions were made following a dispute as to the entitlement to remit.

168.In *An Bord Bainistíochta, Gaelscoil Moshíológ v Labour Court* [2024] IESC 38, O'Donnell CJ examined the function of a court in an appeal on a point of law. The case concerned an appeal from the Labour Court under section 46 of the Workplace Relations Act 2015 which provides for an appeal on a point of law. The Act provides that the decision of the High Court on such an appeal shall be “*final and conclusive*”. At §64, O'Donnell CJ observed:

“Where the High Court concludes that there is an error of law, the order it may make depends upon the error identified, in the same way as the order this Court or the Court of Appeal may make in an appeal. In some cases, if the court concludes that there has been an erroneous finding of primary fact which led to a conclusion in favour of a party, then the court may allow the appeal and set aside the order made and substitute the order which follows from that conclusion. Similarly, if there is an error of law and the correct understanding and application of the law would lead to the contrary conclusion, then the court is entitled to allow the appeal and substitute that conclusion. There may, however, be circumstances where the error identified cannot lead to the substitution of a final order by the court, and may mean that the case has to be remitted to the primary decision-maker. None of this however, expands the court's jurisdiction to substitute an order it considers appropriate for that made by the primary decision-maker. The order which the court makes on an appeal on a point of law, is still constrained because it is an appeal on a point of law.”

169. Although addressing an appeal on a point of law, where the Court stressed that the merits of the underlying dispute were not a relevant consideration, it appears to me that the Court's identification of a power to remit in a case where the error identified cannot lead to the substitution of a final order by the court must apply equally where that situation arises in an appeal on the record. This is consistent with the reasoning of Simons J in *O'Sheehan* where he identified an implied power to remit where that was necessary in order to avoid undermining the statutory scheme.

170. Insofar as the decision in *NzN* might suggest otherwise, I think that must now be reconsidered in light of the observations of the Supreme Court and *O'Sheehan*. It may be, of course, that the situation will rarely arise in an appeal on the record, where a court has the power to review the evidence before the decision-maker – and any new evidence admitted – and form its own view on the merits. But the statutory scheme clearly envisages that any appeal to the High Court will follow an inquiry by the DPC and the exercise by the DPC of its expertise in determining the issues in that inquiry. Where the appeal is from a decision of an expert body such as the DPC, there may be circumstances where it would be unsafe for the court to form a final view on matters requiring expertise without the benefit of the expert body's decision made in light of all relevant evidence. To do so could undermine the statutory scheme.

171. I note that the DPC through its solicitors indicated that they wouldn't object to any point being pursued in the appeal which was more properly a matter for judicial review, and it did not advance any argument that TikTok's breach of fair procedures claims were irrelevant in this appeal.

172. In the circumstances, it appears to me that if TikTok identifies a breach of fair procedures which could, had it been pursued in judicial review proceedings, have entitled it to a remedy, I should consider whether that is a matter which can be fairly addressed within the framework of this appeal in accordance with the statutory scheme. If not, I will consider whether, notwithstanding the absence of an express statutory power, the matter should be remitted to the DPC for further consideration.

Nature of the Inquiry

173. In addition to the dispute regarding the scope of the appeal, the parties dispute whether the Inquiry itself should be characterised as civil or criminal in nature. TikTok contends that by reference to the criteria in the European Court of Human Rights decision in *Engel*, App No 5100/71, that, having regard to the financial penalties to which it is exposed, the Inquiry must be regarded as criminal in nature. Accordingly, it argues, that the rights of the defence guaranteed under Article 48 of the Charter must be observed. For the purpose of these proceedings, the main focus of this argument was TikTok’s contention that, having regard to the criminal nature of the Inquiry, the DPC had impermissibly reversed the burden of proof.

174. Article 48(1) of the Charter provides that “*everyone who has been charged shall be presumed innocent until proved guilty according to law.*” It mirrors Article 6(2) of the European Convention on Human Rights (“ECHR”).

175. TikTok accepts that the enforcement mechanisms of the GDPR could not all necessarily be regarded as criminal in nature, noting that there are civil remedies for breach of provisions of the GDPR (Transcript Day 3, p. 158). But it argues that the possibility of the imposition of very significant criminal sanctions renders those penalties criminal in nature and, accordingly, the rights of the defence protected by the Charter must be observed before making a finding which might lead to the imposition of such a penalty.

176. The three criteria in *Engel* are summarised as followed in TikTok’s submissions:

- (a) whether national law defines the offence as criminal, disciplinary or both – although this “provides no more than a starting point”;*
- (b) the nature of the offence, which is a factor of greater import; and*
- (c) the degree of severity of the penalty that the person concerned risks incurring.*

177. In circumstances where national law does not define breaches of the GDPR as criminal, TikTok’s emphasis is on the third of these criteria, severity of the penalties. It notes that the criteria are not cumulative. TikTok identifies a number of decisions of the CJEU in which the criteria identified in *Engel* are applied. Case C-481/19, *Consob* concerned a preliminary

reference in which the Italian national court queried whether it was permissible to impose fines for refusal to answer questions in relation to insider trading allegations, where the questions might establish liability for an offence which is criminal in nature. The Court noted that the protections afforded by the ECHR were also provided by the Charter (at §36):

“Furthermore, while the questions referred mention Articles 47 and 48 of the Charter, which enshrine, inter alia, the right to a fair trial and the presumption of innocence, the request for a preliminary ruling also refers to the rights guaranteed in Article 6 of the ECHR. Whilst the ECHR does not constitute, for as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into the EU legal order, it must nevertheless be recalled that, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of EU law. Furthermore, Article 52(3) of the Charter, which provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR, is intended to ensure the necessary consistency between those respective rights without adversely affecting the autonomy of EU law and that of the Court of Justice (see, to that effect, judgment of 20 March 2018, Garlsson Real Estate and Others, C-537/16, EU:C:2018:193, paragraphs 24 and 25).”

178. It summarised the three criteria, mirroring *Engels* (at §42):

“... Three criteria are relevant to assess whether penalties are criminal in nature. The first criterion is the legal classification of the offence under national law, the second is the intrinsic nature of the offence, and the third is the degree of severity of the penalty that the person concerned is liable to incur (judgment of 20 March 2018, Garlsson Real Estate and Others, C-537/16, EU:C:2018:193, paragraph 28).”

179. While stipulating that it was a matter for the national court to determine whether the sanctions were criminal in nature, the court observed that the fines which could be imposed in that case, between €10,000 and €5,000,000, “... appear to pursue a punitive purpose and to present a high degree of severity such that they are liable to be regarded as being criminal in nature.”

180.Applying the same criteria, the CJEU determined in Case C-544/19, *Ecotex*, that fines imposed for breaches of a law governing restrictions of cash payments in Bulgaria, an anti-money laundering law, were criminal in nature.

181.Of most relevance for the purpose of these proceedings are the observations of the Advocate General in Case C-683/21, *NVSC*, a case concerning alleged breaches of the GDPR in connection with a Covid mobile phone application in Lithuania. The decision is discussed below in relation to whether there is a requirement for “fault” for the imposition of an administrative sanction under the GDPR. In discussing that issue, the Advocate General commented as follows:

“73. Third, I note that the fines imposed in application of Article 83 of the GDPR can result in severe punishment. Indeed, the first tier, which is covered by Article 83(4) of that regulation, can lead to the imposition of fines of up to EUR 10 000 000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The second tier provides for fines up to EUR 20 000 000 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (again, whichever is higher).

74. Consequently, it would seem to me that the fines imposed in application of Article 83 of the GDPR pursue a punitive purpose, at least in some situations,³⁹ and present a high degree of severity such that they are liable to be regarded as being criminal in nature and, thus, as falling within the scope of Article 49 of the Charter of Fundamental Rights of the European Union (‘the Charter’).”

182.The Advocate General in Case C-768/21, *TR v Land Hessen* made similar observations (at §77).

183.As noted, TikTok claims that the characterisation of the administrative fines which can be imposed under the GDPR is relevant to its argument that the DPC impermissibly reversed the burden of proof. It also suggested that it had a bearing on its fair procedures grounds (Transcript Day 4, p. 19), but no particular argument was advanced that the fair procedures

necessitated in GDPR inquiries were more extensive than suggested by the case law on which TikTok itself relied.

184. The DPC did not engage in detail on TikTok’s argument that the GDPR sanctions are criminal in nature. In its Statement of Opposition, it denied that they were criminal, a fact which TikTok suggests meant that they approached the Inquiry on a mistaken basis. In its written submissions, it noted that there was no authority for the proposition that the GDPR fines should be regarded as criminal, still less that the DPC’s ‘*non-fine*’ analysis should be assessed by some criminal standard.

185. In oral submissions, the DPC did not make further submissions on the question of whether the fines could be regarded as criminal in nature, but noted that there was no absolute prohibition on a reversal of the burden of proof. Counsel referred to Council of Europe guidance, submitted by TikTok, which noted, by reference to case law of the European Court of Human Rights that “*presumptions of fact or of law operate in every criminal-law system and are not prohibited by the Convention*”. The document concludes with a reference to the decision in *Janosevic v Sweden*, Application No. 34619/97 (at §101):

“In Salabiaku, cited above, the Court pointed out (p. 15, § 28):

“Article 6 § 2 does not ... regard presumptions of fact or of law provided for in the criminal law with indifference. It requires States to confine them within reasonable limits which take into account the importance of what is at stake and maintain the rights of the defence.”

Thus, in employing presumptions in criminal law, the Contracting States are required to strike a balance between the importance of what is at stake and the rights of the defence; in other words, the means employed have to be reasonably proportionate to the legitimate aim sought to be achieved.”

186. Having regard to the size of the administrative fines which can be imposed under the GDPR – I note that in this particular case, the fines imposed on TikTok were less than 1% of the maximum which could have been imposed – and the observations of the Advocates General in *NVSC* and *TR v Land Hessen*, it would appear that the imposition of such fines should be regarded as the imposition of a criminal sanction. The DPC did not identify a

basis for contending otherwise. I will, accordingly, consider TikTok's arguments, in particular its argument that there has been an impermissible reversal of the burden of proof, through that prism.

Grounds of appeal

187. TikTok has appealed the Decision on a variety of grounds. In its written submissions, it provides the following helpful summary of those grounds:

1) The Decision was made in breach of TTI's right to fair procedures and legitimate expectations, where the DPC:

(a) made new and materially different adverse findings in the Decision without putting them to TTI and affording it a right to be heard in response;

(b) failed to have adequate regard to the submissions made and evidence adduced by TTI during the Inquiry;

(c) failed to communicate its provisional view on Clover during the Inquiry, or provide TTI with any right to be heard in respect of same;

(d) altered the temporal scope of the Inquiry ("Temporal Scope") without notice or explanation;

(e) refused TTI access to the Inquiry file.

2) The DPC committed a manifest error of assessment in finding that TTI had failed to assess the application of Relevant Chinese Laws to the Temporary Data.

3) In finding an infringement of Article 46 and making the Suspension Order, the DPC erred by failing to carry out the assessment mandated by the CJEU in Schrems II, and relying instead on a negative finding based upon an alleged accountability failure.

4) The DPC erred in engaging in a hypothetical assessment of TTI's entitlement to rely on Article 49 derogations.

5) The DPC misinterpreted Article 13(1)(f) and wrongly found TTI's October 2021 privacy policy to be non-compliant with this provision.

6) The DPC acted ultra vires the Act and Article 83 by imposing administrative fines on TTI where it failed to establish that the infringements found were committed negligently.

7) The DPC acted ultra vires the Act and Article 83, misinterpreted Article 83, and infringed general principles of EU law by imposing administrative fines by reference to the turnover of ByteDance Limited (“ByteDance”).

8) The reasons for the fining decision were wholly inadequate.

9) The DPC made significant errors in its interpretation and application of Article 83.

10) The Decision contains manifest errors of assessment.

11) The DPC misinterpreted Articles 46(1) and 58(2)(i) in making the Suspension Order and erred in making Corrective Orders which are impermissibly vague and provide for an unreasonably short compliance period.

188. During oral submissions, it was confirmed that TikTok was not pursuing Ground 4, relating to Article 49 derogations. It was also stated that it was relying solely on its written submissions in relation to Ground 5, the only appeal ground relating to the finding of a breach of Article 13(1)(f) of the GDPR.

189. In oral submissions some of the remaining grounds were, in broad terms, argued together. In particular, Grounds 1 and 2 were dealt with together, as were Grounds 6, 7, 8 and 9 (relating to the administrative fines). There was some overlap between Grounds 10 and 11 and the other grounds, in particular Ground 3. I propose to address the grounds of appeal directed to the Article 46 infringement and the corrective orders before addressing the sole ground of appeal directed to the Article 13(1)(f) infringement. I will then address Ground 6, one of the grounds of appeal relating to the imposition of the administrative fines.

190. In light of the conclusions in *LinkedIn* regarding the scope of the appeal, careful consideration needs to be given to how the court approaches each ground of appeal. In an appeal on the record pursuant to section 142 and /or 150 of the 2018 Act, the court is entitled to reach its own conclusion in light of the evidence which was before the decision maker, or such additional evidence as the appellant is given leave to adduce. In this case, no

application was made to adduce additional evidence. Some deference may be given to the view of the decision-maker, the DPC, on matters within the sphere of the DPC's technical expertise.

191. In brief terms, Grounds 1 and 2 concern alleged breaches of fair procedures and errors of assessment, whereas Ground 3 pleads errors of law, in effect, that the DPC approached the Inquiry on a misunderstanding of TikTok's, and its own, obligations pursuant to the GDPR. If TikTok is correct about this ground of appeal, then the DPC erred in finding that there was an infringement of Article 46, and, more pertinently, this court could not but find that there had been no breach of Article 46: TikTok's other grounds of appeal against the Article 46 infringement finding and sanction simply would not arise. TikTok also allege that the DPC approached the question of whether to make a corrective order on the basis of a misunderstanding of its legal obligations. The role of the court on this ground of appeal is straightforward, simply deciding which of the parties is correct as a matter of law. For that reason, it seems to me that that is the ground of appeal which should be dealt with first.

Ground 3 – Errors of law

192. TikTok's pleaded complaint under this heading is as follows:

[The] DPC misinterpreted and misapplied Articles 5, 24 and 46 [GDPR], with the result that it erred in law and failed to fulfil its statutory function as LSA.

193. TikTok's overarching complaint under this ground is that the DPC has misunderstood the nature of the obligation imposed on controllers of data by Article 46 of the GDPR. In simple terms, although TikTok accepts that Article 46 imposes on data controllers an obligation not to transfer personal data outside the EU without first *verifying* that the personal data is subject to the equivalent protection guaranteed within the EU, it contends that there is no obligation on data controllers to be able to *demonstrate* that that is so, *i.e.* to stand over its verification. The DPC's decision is clearly framed as a failure by TikTok to "*verify, guarantee and demonstrate*" that the data transferred to China was afforded an equivalent level of protection. It does not, therefore, dispute that it has interpreted Article

46 as imposing such an obligation, rather it argues that this is the correct interpretation. Both parties rely heavily on the decision of the CJEU in *Schrems II*.

194. TikTok advances its general point by reference to four separate arguments. It alleges that the DPC failed to carry out the assessment mandated by the decision of the CJEU in *Schrems II*. Second, it contends that the DPC impermissibly reversed the burden of proof in the Inquiry. Third, it contends that the DPC misapplied the accountability obligation contained in Articles 5(2) and 24(1) of the GDPR. And fourth, it argues that the DPC failed to carry out an adequate risk assessment when analysing the transfers the subject of the Inquiry. In its written legal submissions, it also includes an argument under this heading that the DPC failed to have regard to the supplementary measures in finding an infringement of Article 46(1). However, it seems to me that this is an issue which falls to be considered under Grounds 1 and 10, where it was addressed during oral submissions.

195. The first of the arguments, relating to the decision in *Schrems II*, is central to the complaints TikTok advances in these proceedings and is inter-linked with the second and third arguments. The dispute between the parties can be expressed in simple terms. TikTok contends that in order for the DPC (or any supervising authority) to establish a breach of Article 46 of the GDPR, it must prove that data transferred to a third country is *in fact* not afforded an essentially equivalent level of protection to that guaranteed in the EU. It says that there was no such finding here, indeed no investigation of the level of protection afforded to the personal data transferred to China, other than by reference to the information TikTok provided, and therefore no basis for the finding of a breach of Article 46.

196. The DPC contends that Article 46 imposes a positive obligation on a controller to ensure that essentially equivalent protection is afforded in the third country before it can transfer personal data from the EU to that country. Accordingly, if a controller cannot *demonstrate*, when called upon to do so, that there *is* such equivalent protection, it is not entitled to transfer data to that third country, and if, as here, it has transferred or is transferring data, that constitutes a breach of Article 46.

197. The starting point for this argument is, of course, the GDPR itself, but the parties' arguments were largely focussed on the decision in *Schrems II*, and what the CJEU had said about the obligations on controllers and supervising authorities imposed by Article 46.

Before addressing the parties' arguments, it is worthwhile, therefore, to consider that decision in a little detail.

The decision in *Schrems II*

198. It is important to recall the context for *Schrems II*. As set out above, *per* Article 45 of the GDPR, personal data can be transferred to a third country where the Commission has made an adequacy decision that the data transferred to that country is afforded an equivalent level of protection to that guaranteed in the EU. The applicant, Mr Schrems complained to the DPC that Facebook Ireland was transferring his data to the United States in reliance on a Commission adequacy decision in respect of personal data transferred to the United States, Commission Decision 2000/520/EC (“**the Safe Harbour Decision**”), but that his data was not, in fact, afforded equivalent protection to that guaranteed in the EU. The DPC refused to entertain the complaint, considering that it was bound by the Safe Harbour Decision. Mr Schrems challenged this refusal in High Court proceedings, and the court referred questions to the CJEU regarding, *inter alia*, whether the DPC was “*absolutely bound*” by an adequacy decision or whether it was required to investigate the matter in the light of factual circumstances since the making of the Safe Harbour Decision.

199. In *Schrems I*, the CJEU concluded that the DPC was not precluded from considering the complaint. Importantly, it also concluded that the Safe Harbour Decision was invalid. Mr Schrems' complaint was thus remitted to the DPC for further consideration.

200. Following the declaration by the CJEU in the judgment in *Schrems I* that the Safe Harbour Decision was invalid, transfers of personal data to the United States continued on the basis of other legal provisions. In particular, data-exporting companies made use of contracts with data importers, incorporating standard contractual clauses drawn up by the Commission in Decision 2010/87/EU (“**the SCC Decision**”). The SCC Decision was made under the equivalent of Article 46(2)(c) of the GDPR, which allows for the Commission to adopt standard data protection clauses which provide a mechanism for transfers where there is no adequacy decision. Accordingly, the DPC asked Mr Schrems to reformulate his complaint, which he did.

201. In addition, the Commission made a further adequacy decision, Implementing Decision (EU) 2016/1250 (“**the Privacy Shield Decision**”), which provided a set of rules, oversight mechanisms, and redress procedures intended to safeguard EU citizens’ data when processed in the US.

202. Before the DPC, Mr Schrems argued that these decisions were also invalid having regard to the level of protection actually afforded to personal data in the US, focussing, in particular, on the possibility of public authority surveillance of the data enabled by US laws.

203. Following a detailed investigation by the DPC, in which it considered provisionally that US law does not offer effective remedies in accordance with Article 47 of the Charter to Union citizens, it issued High Court proceedings for the purpose of securing a reference to the CJEU on the validity of the SCC Decision, considering that it was otherwise impossible to adjudicate on Mr Schrems’ complaint. Following a further hearing by the High Court, in which it heard detailed evidence in order to determine whether it shared the concerns of the DPC (as required by *Schrems I*), the court, having concluded that it did share the DPC’s concerns, referred further questions to the CJEU regarding the validity, in particular, of Decision 2010/87/EU. This led to the decision in *Schrems II*. In that decision, the CJEU considered the validity of both the SCC Decision and the Privacy Shield Decision. The CJEU found that the SCC Decision was valid but declared the Privacy Shield Decision invalid. However, it is what the court had to say regarding the duties on controllers and supervising authorities when transferring data to a third country pursuant to Chapter V of the GDPR which was the focus of the parties’ attention in these proceedings.

204. The parties both referred to the opinion of the Advocate General. The sixth question referred queried the level of protection which required to be afforded to personal data transferred to a third country. The Advocate General observed (at §115):

“Like the DPC, Mr Schrems and Ireland, I consider that the ‘appropriate safeguards’ provided by the controller or processor to which Article 46(1) of the GDPR refers must ensure that the rights of the persons whose data are transferred benefit, as in the context of a transfer based on an adequacy decision, from a level of protection essentially equivalent to that which follows from the GDPR, read in the light of the Charter.”

205.He continued (at §117):

“Articles 45 and 46 of the GDPR are aimed at ensuring the continuity of the high level of protection of personal data ensured by that regulation when they are transferred outside the European Union. In fact, Article 44 of the GDPR, entitled ‘General principle for transfers’, opens Chapter V, on transfers to third countries, by announcing that all the provisions in that chapter are to be applied in order to ensure that the level of protection guaranteed by the GDPR is not undermined where data are transferred to a third State. That rule is designed to ensure that the standards of protection resulting from EU law are not circumvented by transfers of personal data to a third country for the purpose of being processed there. Having regard to that objective, it is immaterial that the transfer is based on an adequacy decision or on guarantees provided by the controller or processor, in particular by means of contractual clauses. The requirements of protection of fundamental rights guaranteed by the Charter do not differ according to the legal basis for a specific transfer.”

And at §126 and §127

“In those circumstances, as Mr Schrems and the Commission have observed, the contractual mechanism set out in Article 46(2)(c) of the GDPR is based on responsibility being placed on the exporter and, in the alternative, the supervisory authorities. It is on a case-by-case basis, for each specific transfer, that the controller or, failing that, the supervisory authority will examine whether the law of the third country of destination constitutes an obstacle to the implementation of the standard clauses and, therefore, to an adequate protection of the transferred data, so that the transfers must be prohibited or suspended.

In the light of those observations, I consider that the fact that Decision 2010/87 and the standard contractual clauses which it sets out are not binding on the authorities of the third country of destination does not in itself render that decision invalid. The compatibility of Decision 2010/87 with Articles 7, 8 and 47 of the Charter depends, in my view, on whether there are sufficiently sound mechanisms to ensure that transfers

based on the standard contractual clauses are suspended or prohibited where those clauses are breached or impossible to honour.”

206. Accordingly, the focus was on whether there was a risk that transfers *would not* be suspended even though the SCCs were breached or impossible to honour. If so, that would render the SCC Decision invalid.

207. When considering the eighth question referred, whether a supervisory authority is *required* to use its powers to suspend transfers where it considers that an equivalent level of protection is not guaranteed, the Advocate General concluded that it was. Because there was such an obligation, he concluded that the SCC Decision was valid. He considered first the obligation on controllers:

“134. I believe it is necessary to make a few points here about the content of the examination which the parties to the contract should carry out in order to determine, in the light of the footnote referring to Clause 5, whether the obligations which the law of the third State imposes on the importer entail a breach of the standard clauses and thus prevent the transfer from being accompanied by appropriate safeguards. That issue has been raised, in essence, in the context of the second part of the sixth question.

135. Such an examination entails in my view a consideration of all of the circumstances characterising each transfer; which may include the nature of the data and whether they are sensitive, the mechanisms employed by the exporter and/or the importer to ensure its security, the nature and the purpose of the processing by the public authorities of the third country which the data will undergo, the details of such processing and the limitations and safeguards ensured by that third country. The factors characterising the processing activities carried out by the public authorities and the safeguards applicable in the legal order of that third country may, in my view, overlap with those set out in Article 45(2) of the GDPR.”

208. He then turned to the obligations on supervisory authorities:

“140. The following reasons lead me to consider that, as Mr Schrems, Ireland, the German, Austrian, Belgian, Netherlands and Portuguese Governments and the EDPB

submit, under Article 58(2) of the GDPR the supervisory authorities are required, when they consider following a diligent examination that data transferred to a third country do not benefit from appropriate protection because the contractual clauses agreed are not complied with, to take adequate measures to remedy that illegality, if necessary by ordering suspension of the transfer.

...

144. In the second place, contrary to a further submission of the DPC, the exercise of the powers to suspend and prohibit transfers set out in Article 58(2)(f) and (j) of the GDPR is no longer merely an option left to the supervisory authorities' discretion. That conclusion follows, in my view, from an interpretation of Article 58(2) of the GDPR in the light of other provisions of that regulation and of the Charter, and also from the general scheme and the objectives of Decision 2010/87.

145. In particular, Article 58(2) of the GDPR must be read in the light of Article 8(3) of the Charter and Article 16(2) TFEU. In accordance with those provisions, compliance with the requirements entailed by the fundamental right to protection of personal data is subject to review by independent authorities. That task of monitoring compliance with the requirements relating to the protection of personal data, which is also referred to in Article 57(1)(a) of the GDPR, entails an obligation for the supervisory authorities to act in such a way as to ensure the proper application of that regulation.

146. Thus, a supervisory authority must examine with all due diligence the complaint lodged by a person whose data are alleged to be transferred to a third country in breach of the standard contractual clauses applicable to the transfer. Article 58(1) of the GDPR confers on the supervisory authorities, for that purpose, significant investigative powers.

147. The competent supervisory authority is also required to react appropriately to any infringements of the rights of the data subject which it has established following its investigation. In that regard, each supervisory authority has, under Article 58(2) of the GDPR, a wide range of means — the various powers to adopt corrective measures listed in that provision — of carrying out the task entrusted to it.”

209.In its judgment, the court confirmed the Advocate General's view that the level of protection afforded in a third country must be essentially equivalent to that guaranteed within the EU by the GDPR read in light of the Charter. The assessment required by Article 46(1) was also considered (at §104):

“The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, 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. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.”

210.The court also agreed that a supervisory authority was required to suspend transfers where adequate protection cannot be guaranteed and where the controller or processor has not itself put an end to the transfers (at §113 and §121).

211.In considering the validity of the SCC Decision, the court considered the obligations on controllers and supervising authorities:

“133 It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

134 In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the

responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

135 Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such 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. 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.

...

142 It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient 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.”

Alleged misinterpretation of the GDPR

Arguments

212. TikTok’s first and third arguments, both of which relate to the proper interpretation of the GDPR, can conveniently be dealt with together.

213. TikTok contends that it has fulfilled its obligation under Article 46 by carrying out the various data transfer assessments. Even if the court accepts that the DPC was entitled to conclude as a matter of *fact* that those assessments were inadequate, it contends, by reference to *Schrems II*, that before the DPC could make any finding of infringement or impose any sanction on it, it was required to carry out its own assessment of whether the data the subject of the transfers being investigated was subject to essentially equivalent levels of protection in the third country. It refers to this as “*the assessment mandated by Schrems II*”. Since it is not in dispute that the DPC did not carry out such an inquiry, TikTok argue that it erred in law in imposing the administrative fine and making the suspension order.

214. TikTok contrasts the nature of the investigation in this case with that carried out by the DPC which was the subject of the decision in *Schrems II*. In that instance, the DPC carried out a detailed investigation into the level of protection afforded to personal data by US law. In this case, the DPC did not carry out *any* independent assessment of Chinese law; indeed, it expressly stated in the Decision that it was taking the information provided by TikTok regarding the legal position in China “*at its height, and at face value, with regard to its veracity*” in circumstances where TikTok had confirmed that the legal analysis contained in Section 2 of the DTAs had been prepared by one of China’s leading independent law firms. This, suggests TikTok, was an abdication by the DPC of its responsibility as supervising authority.

215. TikTok highlights a number of features of *Schrems II*, which they characterise as “*the definitive decision in relation to data transfer and the requirements of Chapter V*” (Transcript, Day 10, p. 130). It highlights that, at paragraphs 134 and 142 of the CJEU’s judgment, the court refers to the obligation on controllers (and processors) to “*verify*” whether a third country provides adequate protection of data. It accepts, therefore, that it was under an obligation to verify that there was an equivalent level of protection, which it claims to have met by preparing its DTAs, but distinguishes this from an obligation to demonstrate, which it argues is not imposed by the GDPR, as interpreted in *Schrems II*. It notes that both ‘verify’ and ‘demonstrate’ are terms used within the GDPR and that they must, accordingly, be afforded different meanings. It emphasises the passages in *Schrems II* which refer to the obligation on a supervisory authority to suspend transfers where, *having carried out an examination*, it concludes that essentially equivalent protection cannot be

guaranteed. It concludes, therefore, that *Schrems II* is authority for the proposition that a supervising authority can only suspend transfers, or make a finding of infringement, after it has first reached such a conclusion.

216. TikTok also argues that the DPC erred by interpreting Article 46 of the GDPR in light of Articles 5(2) and 24(1) of the GDPR. It notes that Article 5(2) relates only to the principles set out in Article 5(1) and therefore has no general application. It describes the obligation identified in Article 24(1) as a “*separate and distinct obligation*” (Transcript Day 10, p. 129, line 2) to that identified in Article 46. It notes that there is no reference to Articles 5 or 24 in *Schrems II*.

217. The DPC also rely on *Schrems II*. Though it highlights that the nature of the proceedings in both *Schrems I* and *Schrems II* was quite different than these proceedings, and that the judgments were addressed to different questions than at issue in the Inquiry, it argues that *Schrems II* makes clear that the responsibility is on controllers (or processors) to ensure that there is an appropriate level of protection when personal data is transferred to a third country. It contends that the obligation identified in *Schrems II* to *verify* adequate protection before transferring data necessarily requires that a controller be able to *demonstrate* that level of protection. It contends that there is no difference between these two concepts.

218. The DPC argues that the requirement to demonstrate compliance flows from Articles 5 and 24 of the GDPR, and there was nothing improper in it having regard to those provisions in interpreting the scope of Article 46.

Discussion

219. This ground of appeal concerns, in essence, the scope of the obligations imposed on controllers by the GDPR. It also imposes obligations on processors, but since this appeal is concerned only with TikTok’s position as controller of personal data, I will refer only to the position of controllers hereafter. TikTok’s argument is first and foremost a question of interpretation of the GDPR itself, though the parties both lean heavily on prior interpretation of the GDPR by the CJEU in *Schrems II*.

220. The GDPR is designed to guarantee certain rights for data users in respect of their personal data. It does so by placing obligations on controllers of personal data and giving supervising authorities powers of investigation and enforcement. The territorial scope of the Regulation is the EEA. In order not to entirely undermine the protections afforded, the GDPR prohibits controllers transferring personal data from within the EEA to third countries, *i.e.* from within to outwith its territorial scope, unless the same level of protection is guaranteed in those third countries (see Recital 101, quoted above). The purpose of this prohibition is to ensure the high level of protection of personal data guaranteed by the GDPR.

221. Article 5(1) of the GDPR sets out the principles on which the GDPR is based. These include that all data is processed lawfully. Article 5(2) imposes an obligation on the controllers of personal data to be able to *demonstrate* compliance with Article 5(1), *i.e.* to be able to demonstrate that data is being processed lawfully. The requirement that controllers be able to demonstrate that their processing of personal data is lawful is, accordingly, one of the foundational principles of the GDPR.

222. Similarly, Article 24 of the GDPR imposes a “*general obligation*” on controllers to be able to demonstrate that their processing of data is in accordance with the requirements of the GDPR.

223. The general principle in relation to transfers to a third country, the subject of Chapter V of the GDPR, is set out in Article 44 of the GDPR. It is expressed to be “*subject to the other provisions of this regulation*”. It expressly provides that “*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.*”

224. Article 45 provides for a general mechanism to enable transfers, the making of adequacy decisions by the Commissions. As set out in *Schrems II* (at §162):

“*In order for the Commission to adopt an adequacy decision pursuant to Article 45(3) of the GDPR, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order.*”

225. As an alternative, a controller may transfer data in the absence of an adequacy decision where the provisions of Article 46 are satisfied. Just as an adequacy decision can only be made where there is an equivalent level of protection guaranteed, it is obvious that a transfer can only be made pursuant to Article 46 where equivalent reassurance is ensured to that provided by an adequacy decision. *Schrems II* makes clear that, irrespective of the mechanism relied on for a transfer, the same level of protection, essentially equivalent to that provided in the EEA, must be guaranteed.

226. TikTok accept that it was required to assess the level of protection afforded to data in China and only transfer data where it had verified that effectively equivalent protection was guaranteed. The nature of the assessment it was required to set out is described at §135 of the Advocate General's opinion and §104 of the CJEU's judgment, set out above.

227. Where the parties differ is in TikTok's contention that once it had satisfied *itself* that there was equivalent protection, it must be taken to have complied with Article 46 unless the DPC proved that there was not, in fact, essentially equivalent protection. The DPC contend that it was entitled to consider the *adequacy* of TikTok's assessment. Where the assessment was lacking, because it didn't demonstrate that there was adequate protection afforded to data transferred to China, the DPC was entitled to conclude that TikTok had infringed Article 46. Both a literal and purposive interpretation of the GDPR support the DPC's interpretation. It is difficult to find anything in the wording of Chapter V, the GDPR more generally, or *Schrems II*, which supports TikTok's narrow interpretation .

228. Turning first to *Schrems II*, which was the focus of TikTok's submissions on this point, TikTok have, in my view, read far too much into what is said in *Schrems II* in relation to the obligations on supervising authorities.

229. As noted above, *Schrems II* was addressed to an entirely different factual scenario than that at issue here. There was no issue regarding the adequacy of any step taken by the controller of data in that case, Facebook, only with the validity of Commission adequacy decisions on which it relied. The examination of the role of controllers and supervising authorities was carried out for the purpose of determining the validity of the SCC Decision, not for the purpose of any issue arising from an Article 46 assessment by Facebook.

230. The eighth question referred in *Schrems II* concerned the question of the discretion afforded to supervising authorities where, following an investigation, it had concluded that essentially equivalent protection could not be guaranteed. As noted above, both the Advocate General and the CJEU concluded that the SCC Decision was valid because if a supervising authority, following an examination, concluded that essentially equivalent protection could not be guaranteed, it would be required to suspend any transfers.

231. The parties agree that the conclusion is premised on a finding of infringement. TikTok accuse the DPC of a “*leap, not supported by logic*” of saying that one can disregard what’s said in response to question 8, because, it claims, the DPC ignores what is said by the CJEU in response to question 8 simply because it is not addressing the question of whether there must be a prior investigation by the DPC. With respect, it is TikTok’s reliance on the response to question eight which is of questionable logic.

232. The CJEU determined that *if* a supervising authority carries out an investigation and concludes that essentially equivalent protection cannot be guaranteed by the use of the standard data protection clauses in the SCC Decision, it must suspend the transfers. It is logical to infer that if *for any reason*, a supervising authority concludes that essentially equivalent protection cannot be guaranteed, then the same obligation to suspend arises. However, the corollary of that proposition is *not* that that is the only circumstance in which a supervising authority can take any corrective action, still less that a supervising authority must carry out its own assessment of the level of protection where a controller fails to complete an adequate assessment. The fact that a supervising authority must act in a particular way in one set of circumstances does not translate to that being the only circumstance in which the supervising authority can act at all. There is no support in *Schrems II* for TikTok’s overarching argument that a supervising authority cannot make a finding of infringement without having first carried out an investigation and then concluded that there is not equivalent protection in the third country to which data is being transferred.

233. As noted above, *Schrems II* does expressly state that a controller must verify, prior to transfer, that the appropriate level of protection is available (see §134 and §142), and the DPC seek to interpret that as confirming its view that a controller must be able to demonstrate the adequacy of protection. Apart from the obvious point, that an obligation to

verify would be rendered sterile if the obligation was not to carry out an *adequate* verification, and if the adequacy of the verification could not be tested, the judgment does not provide express guidance on the nature of that obligation or, more importantly, the role of supervising authorities in policing it.

234. I accept what both parties say regarding the importance of *Schrems II* in understanding the obligations imposed by the GDPR and certainly it provides assistance in addressing the issues before this Court. But it does not directly answer the question at issue here for the simple reason that neither that question, nor anything analogous to it was before the Court.

235. If the answer can't be found in *Schrems II* as the parties suggest – because the issue simply didn't arise on the facts or on the basis of any of the questions referred – then it is to the GDPR we must turn when considering TikTok's argument.

236. First, it must be observed that the mechanisms in Articles 45 and 46 *facilitate* controllers to do that which would otherwise be impermissible. The starting point is that controllers of personal data have certain obligations in relation to personal data under their control and are simply not permitted to transfer personal data outside the EEA unless certain criteria are met. It is, accordingly, entirely unsurprising that the GDPR imposes an obligation on controllers to establish that they satisfy those criteria if they wish to do what would otherwise be impermissible. It is difficult to understand how the GDPR could be effective were it otherwise.

237. Such a requirement is built into Article 46, which expressly provides that a controller can only transfer data where the controller has provided appropriate safeguards and effective protection is available. Plainly this requires a *prior* assessment of the level of protection afforded to personal data in the third country, as confirmed in *Schrems II*. Moreover, it is for the controller to ensure that the safeguards are put in place.

238. There is nothing subjective about the requirement that essentially equivalent protection be afforded. Again unsurprisingly, the GDPR does not provide that the controller's reasonable belief that there is essentially equivalent protection is sufficient to enable transfers to third countries to take place; such would hardly provide the high levels of protection guaranteed by the GDPR. Moreover, it is clear that the controller is, or should be,

the party with the relevant means of knowledge regarding the transfers, *i.e.* the party in a position to identify appropriate safeguards having regard to the nature and purpose of the transfers it proposes to make.

239. Article 46 must also be read in the context of the general obligation identified in Article 44. That provision is expressly stated to be “*subject to the other provisions of the Regulation.*” Its purpose is to ensure that the protections afforded by the GDPR are not undermined. In that context, in the Decision, the DPC concluded that Article 46 should be read in light of Articles 5(2) and 24(1) of the GDPR, which impose obligations on controllers to be able to demonstrate the lawfulness of any data processing and their compliance with the GDPR. TikTok argues either that these provisions are irrelevant for the purpose of interpreting Article 46 or, perhaps in the alternative, that the DPC erred by making a finding of a breach of Article 46 when, in fact, its conclusion was that there was a breach of Article 24(1). For the purpose of addressing this ground of appeal, it is not necessary to address TikTok’s argument that neither provision was, *in fact*, breached. As TikTok points out, there is a significant legal implication to concluding that there was a breach of Article 46 rather than Article 24, because the GDPR makes no provision for imposing administrative fines in respect of a breach of Article 24.

240. It is very difficult to understand the basis upon which TikTok contends that Articles 5(2) and 24(1) are not relevant to the interpretation of Article 46. They manifestly are. The first is described as a general principle, the second a general obligation. They should both be understood, therefore, absent some very clear indication to the contrary, as applying to all the provisions of the GDPR. Rather than an indication to the contrary, Article 44 expressly provides that the obligations in Chapter V are subject to all other provisions of the GDPR. Thus, on a plain reading of the Regulation, the specific obligation in relation to transfers of personal data to third countries – not to do so unless there are adequate protections in place in the third country – must be read in light of the general obligation on a controller to be able to demonstrate compliance with the GDPR, and subject to the general principle that a controller must be in a position to demonstrate the lawfulness of its processing.

241. TikTok’s arguments to the contrary must be rejected. It says that Article 5(2) has no relevance since it is confined to demonstrating compliance with Article 5(1). But that

doesn't assist TikTok at all: Article 5(1) requires that data be processed lawfully. A requirement to be able to demonstrate compliance with Article 5(1) necessarily, therefore, imports a requirement to be able to demonstrate that all personal data is processed lawfully, regardless of how it is processed. TikTok does not dispute that the transfers to China involve processing for the purpose of the GDPR, nor did it identify any plausible basis for contending that the principle identified in Article 5, that a controller be able to demonstrate the lawfulness of its processing, does not apply to processing pursuant to Article 46.

242. TikTok described the obligation in Article 24(1) as a “*separate and distinct obligation*” (Transcript Day 10, p. 129, line 2) to the obligation in Article 46. This is plainly not the case. It is expressly stated to be a general obligation. There is nothing in the text of Article 24(1) or Chapter V of the GDPR which suggests that the processing to which it relates somehow excludes the processing regulated by Article 46. No reading or interpretation of the GDPR supports such a conclusion.

243. If the specific obligation imposed by Article 46 is read in light of the general obligation imposed by Article 24(1), this means that Article 46 incorporates an express obligation that a controller be able to demonstrate compliance with the requirements of Chapter V, at least when called upon to do so. An inability to demonstrate compliance is a breach of Article 46, not simply a breach of Article 24(1). There was thus no error of law by the DPC in concluding that there was a breach of Article 46 when read in light of Article 24(1). Article 24(1) is not a stand-alone obligation at all, rather it is an obligation which is read into all the other relevant obligations in the GDPR, hence, perhaps, no provision is made for imposing a fine for breach of that obligation.

244. TikTok also suggest that Articles 5 and 24 must have no relevance because they are not referenced in *Schrems II*. But as explained when considering TikTok's first limb of arguments, this is amply explained by fact that Facebook's obligations were not in issue in *Schrems II*. In that case, Facebook had relied on the SCC Decision and the Privacy Shield Decision. There was simply no argument that even if these were valid, Facebook had somehow fallen short in discharging its verification obligations when transferring data to the United States. The fact that these provisions are not relied on in *Schrems II* is, accordingly, of no significance.

245. I note that guidance published by the EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0* (“**the EDPB Supplementary Measures Recommendations**”) also reads Article 46 in light of the accountability obligations in the GDPR (at §3 and §4):

The right to data protection has an active nature. It requires exporters and importers (whether they are controllers and/or processors) to go beyond an acknowledgement or passive compliance with this right. Controllers and processors must seek to comply with the right to data protection in an active and continuous manner by implementing legal, technical and organisational measures that ensure its effectiveness. Controllers and processors must also be able to demonstrate these efforts to data subjects and data protection supervisory authorities. This is the so called principle of accountability.

The principle of accountability, which is necessary to ensure the effective application of the level of protection conferred by the GDPR also applies to data transfers to third countries since they are a form of data processing in themselves. As the Court underlined in its judgment, a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR read in the light of the Charter must 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.

246. Standing back, it is immediately obvious that on TikTok’s argument, taken to its logical conclusion, Article 46 places no real obligation on controllers at all, or at least none which they could be found to have infringed, notwithstanding that Article 83 clearly provides that administrative fines *can* be imposed for infringement of Article 46. Since controllers are not entitled to process personal data other than in compliance with the GDPR, the obligation not to transfer personal data to third countries where there is inadequate protection adds nothing to a controller’s obligations if it is not under a prior duty to adequately ensure that there is such protection. If the adequacy of its discharge of that obligation cannot be tested to ensure that it has been complied with, then it is no obligation at all.

247. In an effort to avoid the logic of its own argument, TikTok accepts that a controller has an obligation to *verify* adequate levels of protection: in oral argument, counsel noted that in *Schrems II*, the controller’s obligation was “*framed in terms of verifying and guaranteeing*”

(Transcript Day 3, pp. 109/110). It also accepted, in argument, that a failure to *attempt* to verify would constitute a breach of article 46, but suggests that if a controller has “*engaged prima facie in the analysis*” required to verify the level of protection, the controller will have discharged its duty (Transcript Day 3, p. 113). On TikTok’s view, ‘verification’ is entirely distinct from ‘demonstration’ and all that is required to verify is for a controller to satisfy *itself* that there are adequate levels of protection, although it accepts that it is required to record this verification, which it does in its DTAs.

248. The difficulty for TikTok is that there is no support in *Schrems II*, still less in the GDPR itself, for such an analysis. TikTok’s only argument is that by the use of the term “*verify*” in *Schrems II*, the CJEU must be taken to have concluded that there was no obligation in the GDPR to be able to demonstrate that it had verified. There is nothing in *Schrems II* which suggests that that is what the court intended. Neither a literal, nor a purposive interpretation of the GDPR supports such a proposition. TikTok’s argument that the terms *verify* and *demonstrate* are both used in different contexts in the GDPR, suggesting that they must be given different meanings, does not assist TikTok at all: neither are used in Article 46. The words used in Articles 5(2) and 24 are ‘*able to demonstrate*’.

249. Once TikTok accepts, as it must, that there is *an* obligation imposed on it by Article 46 to carry out an assessment in respect of transfers of personal data outside the EU, the implausibility of its position becomes obvious. If there is a requirement to carry out such a prior assessment, which there manifestly is, it must be a requirement to carry out an *adequate* assessment. TikTok’s apparent view is that once a controller has satisfied itself that its assessment is adequate, the only means by which a supervising authority can establish a falling short on the part of the controller is, in effect, to carry out its own assessment and show that the controller’s conclusion is wrong. It is true that a supervising authority *could* establish a breach of Article 46 by showing that, in fact, essentially equivalent protection is not guaranteed in the third country, but that it is not the only means of so doing. It is also open to a supervising authority to examine the assessment carried out by a controller and consider whether it was adequate, and whether it in fact demonstrates what it purports to demonstrate. Where, as here, the supervising authority identifies a gap or shortcoming in that assessment, it is entitled as a matter of law to conclude that the controller has not complied with its obligations under Article 46. Insofar as TikTok suggests that this imposes an unfair burden on a controller, and exposes it to significant sanctions, I

do not accept that this is so. As discussed below in relation to Ground 6, a supervising authority will only be entitled to impose a fine where it concludes that any failing was negligent or intentional. Insofar as a supervising authority may impose other forms of order, such as the suspension order here, it must, as I conclude below, first carry out some assessment of the proportionality of so doing. Where it concludes, based on all the information provided by a controller, that the risk of infringement of data users' fundamental rights warrants a suspension order, a controller can hardly rely on its own inadequate assessment to complain that such suspension is unfair.

250. TikTok's interpretation is also unworkable in practice. It would, in effect, require supervising authorities to assess the level of protection provided to personal data in all third countries to which personal data is transferred from the EU. Moreover, they would have to do it in respect of every type of transfer which was taking place. This is an administrative burden which would simply be overwhelming, and all to facilitate those who wish to transfer personal data outside the region in which the protection afforded by the GDPR is available. The result, inevitably, is that the purpose of the GDPR would be grossly undermined. TikTok's vision of the GDPR as imposing obligations on *supervising authorities* rather than *controllers* must be rejected, on this ground at least.

Alleged reversal of burden of proof

Arguments

251. TikTok also argues that the DPC reversed the burden of proof by requiring it to prove compliance with Article 46, and, in effect, made a presumption of guilt in requiring TikTok to demonstrate that the personal data transferred to China was subject to essentially equivalent protection to that guaranteed in the EU. In this regard, TikTok relies on its contention that, having regard to the severity of the sanctions imposed by the GDPR, it is entitled to the benefit of the procedural rights guaranteed in criminal proceedings and that a reversal of the burden of proof is impermissible.

252. TikTok refers to Case T-141/08, *E.ON Energie v European Commission* as an example of a regulator impermissibly reversing the burden of proof. In that case, the Commission carried out an inspection at the applicant's premises for the purpose of investigating a competition law complaint. It sealed the premises pending completion of the inspection, but when it returned the seal had been broken. Following an investigation, the Commission made a finding that the applicant had broken the seal and "*at least negligently*" infringed the relevant Regulation. It imposed a fine of €38 million. The applicant sought to annul that decision claiming, *inter alia*, that the Commission had failed to have regard to the burden of proof. TikTok references the following from the General Court's judgment (at §48):

"Under Article 2 of Regulation No 1/2003 and according to settled case-law relating to the application of Articles 81 EC and 82 EC, in the field of competition law, where there is a dispute as to the existence of an infringement, it is for the Commission to prove the infringements found by it and to adduce evidence capable of demonstrating to the requisite legal standard the existence of the circumstances constituting an infringement... ... For that purpose, it must gather sufficiently precise and consistent evidence to support the firm conviction that the alleged infringement took place..."

253. And at §74 - §76:

"As was recalled in paragraph 48 above, in the field of competition law, it is for the Commission to prove the infringements found by it and to adduce evidence capable of demonstrating to the requisite legal standard the existence of the circumstances constituting an infringement. For that purpose, it must gather sufficiently precise and consistent evidence to support the firm conviction that the alleged infringement took place.

It should also be noted that, for the purpose of complying with the principle of good administration, the Commission must play its part, using the means available to it, in ascertaining the relevant facts and circumstances ...

The guarantees conferred by the Community legal order include, in particular, the duty of the competent institution to examine carefully and impartially all the relevant aspects of the individual case ..."

254. The DPC argues that it was merely applying the GDPR as interpreted by *Schrems II*. There was, therefore, no error of law by it in its approach to the Inquiry. Any complaint by TikTok is a complaint about the GDPR, not the Decision. The DPC denies, in any event, that there has been any reversal of the burden of proof. Consistent with *E.On Energie*, the legal and evidential burden remained on the DPC to prove that TikTok's assessment of the level of protection afforded to personal data to be transferred to China was inadequate.

Discussion

255. In order to address this argument, it is necessary to understand what TikTok's complaint actually is. It seems to argue that it was required to prove its innocence by demonstrating that data transfers by it to a third country, China, were subject to an equivalent level of protection to that guaranteed within the EU, and that this is impermissible having regard to the criminal sanctions which can be imposed in the event of a finding of infringement. For the purpose of this argument, I accept that the administrative fines which can be imposed under the GDPR, having regard to their severity, should be regarded as criminal in nature.

256. The first, and complete, answer to this complaint is that insofar as TikTok were required to be able to demonstrate anything, that was not an obligation imposed by the DPC, but an obligation imposed by the GDPR, for the reasons explained in the paragraphs immediately above. There was no error by the DPC in interpreting the GDPR as it did. There is no challenge to the GDPR in these proceedings, and therefore, no basis for impugning the DPC's decision on this ground.

257. The only viable argument TikTok could pursue by reference to a purported impermissible reversal of the burden of proof is that such reversal is *always* impermissible and, accordingly, the GDPR must be interpreted in such a way as to ensure that there is no impermissible reversal of the burden of proof. There are a number of difficulties with this argument.

258. First, insofar as I have concluded that the GDPR imposes an obligation on controllers to be able to demonstrate that personal data transferred to third countries is subject to

equivalent levels of protection, that is the only plausible interpretation of the GDPR available. It is consistent with a literal and purposive interpretation of the GDPR, ensuring a high level of protection for personal data. TikTok's contrary interpretation, that it need only satisfy itself that there is sufficient protection, and that it is for the supervising authority to demonstrate that there *isn't* equivalent levels of protection is inconsistent with the express terms of the GDPR, requires the provisions of Articles 5(2) and 24 to be disregarded, and is at odds with the purpose of the GDPR, undermining some of its essential protections.

259. In any event, such reversal is not always impermissible. As discussed above, presumptions of fact and law are a feature of all legal systems and, *per Janosevic*, states are “*required to strike a balance between the importance of what is at stake and the rights of the defence; in other words, the means employed have to be reasonably proportionate to the legitimate aim sought to be achieved.*”

260. But second, and more importantly, I am not satisfied that the finding of an infringement in this case involved a reversal of any burden of proof at all. Article 46 prohibits the transfer of personal data outside the EEA unless certain conditions are met, *i.e.* the controller has ensured or verified that there is essentially equivalent protection afforded to that data in the third country to that guaranteed in the EEA, and is able to demonstrate that that is so. In order for a supervising authority to find an infringement of the GDPR, the supervising authority must prove that the controller has not verified that the data is adequately protected and/or is unable to demonstrate that it is. The legal and evidential burden at all times remained and remains on the DPC. In the case of an inadequate assessment, the DPC must prove that it is inadequate, by showing that it contains errors or by showing that it is incomplete.

261. Though TikTok relies on certain statements of principle in *E.On Energie*, it does not refer to the following:

“55. However, in the same way as, where the Commission relies, in establishing an infringement of Articles 81 EC and 82 EC, on documentary evidence, the burden is on the undertakings concerned not only to put forward a plausible alternative to the Commission's view but also to allege that the evidence relied on in the contested decision to establish the existence of the infringement is insufficient... it must be held that, in a case such as this, where the Commission relies on direct evidence, it is for the

undertakings concerned to demonstrate that the evidence relied on by the Commission is insufficient. It has already been ruled that such a reversal of the burden of proof does not infringe the principle of the presumption of innocence ...”

262. Moreover, it ignores the court’s analysis of what the Commission had actually done and the fact that it rejected the applicant’s complaints. At §85 of the judgment, the court noted that it is was for the Commission to prove the breach of the seal, but it was “*not its responsibility to demonstrate that the room which had been sealed was actually entered or that the documents stored there were tampered with.*”

263. In this regard, it should be recalled that it is undisputed that personal data transferred to China is, absent additional protections, not afforded equivalent protection to that guaranteed within the EEA. That was and is TikTok’s unequivocal position. In those circumstances, two key elements necessary to show an infringement of Article 46, that personal data had been transferred outside the EEA to China, and that personal data is not afforded equivalent protection in China had clearly been established. The only issue, as we will see, is whether, having regard to the particular circumstances of the transfers and the additional measures put in place by TikTok, it could be shown that these particular transfers were, notwithstanding the general position, afforded equivalent protection. The DPC concluded on the evidence that that had not been established. There is nothing impermissible about an inquiry which examines TikTok’s purported verification of its contention that there was equivalent protection and determines whether, as a matter of fact, it shows what TikTok contends. The approach taken by the DPC was consistent with that adopted by the Commission in *E.On Energie*, confirmed to have respected the rights of the defence by the General Court.

264. I note that TikTok’s arguments were focussed on the *burden* of proof and were not addressed to the *standard* of proof, whether on a controller in showing that it has adequately assessed the level of protection on a third country, or on a supervising authority to prove that it had not. In the circumstances of this case where the DPC’s conclusion that TikTok had not, in effect, addressed at all the level of protection for personal data processed in China, it was necessary for the DPC only to prove that there was a material gap in the assessment. As I conclude below, there undoubtedly was. As we will see when discussing

the third Xu opinion, more difficult issues will arise where a controller does appear to address the level of protection available, but in a manner which is unclear or unconvincing.

Alleged requirement to carry out risk assessment

Arguments

265. The final argument advanced by TikTok under this heading relates to a purported requirement on the DPC to carry out a risk assessment both in determining the measures necessary in order to ensure equivalent protection (an argument revisited at Ground 11), and also in determining whether there was an infringement. This plea, accordingly, is addressed to both the infringement finding and the suspension order.

266. The necessity for a risk assessment is an issue which TikTok raised in its response to the PDD. As set out therein, TikTok argue that the requirement for the DPC to assess the risk to data users' rights arises, firstly, from Article 24(1) of the GDPR which imposes a requirement on a controller to put in place appropriate measures “[t]aking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons”, also reflected in Recital 76 of the GDPR. Implicit in this, argues TikTok, is that a controller is only required to put in place measures which are proportionate to the risks posed, not to guarantee no risk whatsoever, however theoretical or remote, and that the DPC was required to assess whether there had been an infringement of Article 46 on that basis.

267. This is confirmed, it argues, by the EDPB Supplementary Measures Recommendations, which the DPC purported to follow.

268. §43.3 of that document sets out:

43.3 The assessment may reveal that relevant legislation in the third country may be problematic and that the transferred data and/or the importer at hand fall or might fall within the scope of this problematic legislation.

In light of uncertainties surrounding the potential application of problematic legislation to your transfer, you may then decide to:

- *Suspend the transfer;*
- *Implement supplementary measures to prevent the risk of potential application to your importer and/or to your transferred data of laws and/or practices of the third country of the data importer, which are capable of impinging on the transfer tool's contractual guarantees of an essentially equivalent level of protection to that guaranteed in the EEA; or*
- *Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below.*

Therefore, you will need to have demonstrated and documented with a detailed report that problematic legislation will not be applied in practice to your transferred data and/or importer, and, consequently, that it will not prevent the importer from fulfilling its obligations under the Article 46 GDPR transfer tool.

269. TikTok notes that the Decision refers, at §511, to the EDPB Supplementary Measures Recommendations but fails to advert to the third bullet point above.

270. TikTok argues that the requirement for a risk-based approach is also supported by *Schrems II* and points to various passages from the CJEU's judgment.

271. In its response to the PDD, TikTok returns to the requirement for a risk-based approach when addressing the corrective measures proposed by the DPC. It contends that the EDPB Supplementary Measures provide that “*where there is no reason to believe that potentially*

problematic laws may be applied in the specific circumstances of a transfer; that transfer may proceed in accordance with the GDPR”, again referring to §43.3 of that document.

272. It identifies a series of factors which it suggests means that there is no actual risk to EEA user data and, accordingly, no basis for making a suspension order, including the evidence from the various legal experts that Chinese authorities had never attempted to access data from companies in a similar position to TikTok, *i.e.* which did not provide a service within China, and that no request had ever been made of TikTok.

273. TikTok argues that the DPC misdirected itself at law by considering that, in the event of an infringement finding, it was obliged to make the suspension order. It refers to the following passage from the Decision (at §261):

In the context of this Inquiry, it is the responsibility of the DPC to review the assessment made by TikTok Ireland in the exercise of its powers under, inter alia, Article 57(1)(a) GDPR, to ascertain whether the transfers the subject of this Inquiry comply with the requirements laid down in the GDPR. The Schrems II judgment makes clear that if TikTok Ireland is not able to guarantee a level of protection essentially equivalent to that guaranteed within the European Union, then the DPC, as the competent supervisory authority is required to suspend or end the transfers if TikTok Ireland has itself failed to suspend or end them.

274. A similar statement is contained at §675 of the Decision.

275. In its written submissions, the DPC does not address this last point, but does contend that it considered the risks to EEA user data in concluding that there was an infringement, *and* when deciding to make the suspension order. Accordingly, notwithstanding its apparent statements at §261 and §675 of the Decision that it was obliged to make the suspension order having concluded that TikTok could not ensure the level of protection guaranteed within the EU, it appears to accept that some form of assessment of whether such an order was necessitated was required.

Discussion

276. It is appropriate first to address the suggestion that the DPC erred in not carrying out a risk assessment to determine whether there had been an infringement at all. In light of its conclusion that TikTok had failed to assess whether there was equivalent protection available, it is difficult to see how the DPC could have reached any conclusion other than that this was an infringement. Where there is an inadequate consideration of the level of protection afforded to personal data in the third country to which personal data is to be transferred, any assessment of risk by the controller is necessarily compromised. I do not rule out the possibility that a supervising authority might nonetheless conclude that there is, in fact, no meaningful risk, but in a case where a controller is transferring very significant amounts of personal data belonging to millions of users, it is very difficult to see any basis upon which the DPC could have said that there was no breach of Article 46. Having determined that there was an infringement, it was, of course, then required to consider whether to impose an administrative fine or make a corrective order, but it could not but have concluded that TikTok had infringed.

277. Despite denying its relevance to the interpretation of Article 46, TikTok relies on Article 24 of the GDPR. This provides, as we have seen that a *controller* take into account the risks to the rights and freedoms of natural persons when designing technical and organisational measures to ensure that processing is performed in accordance with the GDPR. TikTok, correctly in my view, and consistent with the EDPB Supplementary Measures Recommendations, interprets this as allowing a risk-based assessment by a controller in determining what measures to put in place. It *incorrectly* interprets this as imposing an obligation on a supervising authority to carry out that risk assessment where a controller has not done so even for the purpose of finding an infringement. In truth, TikTok's argument in this regard is another manifestation of its complaint that a supervising authority can only make a finding of infringement where it proves that data has been transferred which was not afforded essentially equivalent protection.

278. The risk-based assessment to be conducted by the controller is, necessarily, a prior assessment. By correctly identifying the level of protection available and the risks that any deficit in protection might create for the rights and freedoms of data subjects, a controller can design measures to ensure equivalent protection is guaranteed, decide not to transfer the

data, or decide to transfer the data without further protections where the risk is purely theoretical. It is a necessary pre-requisite to proper decision-making by the controller that it has, in fact, adequately assessed the level of protection. If there is a failure by the controller to do what is required of it, adequately identify the level of protection available, then its risk assessment and design of measures is necessarily compromised. That is sufficient for a supervising authority to determine that there has been an infringement of the GDPR. For that purpose, it is not necessary for a supervising authority to carry out its own risk assessment to determine whether, notwithstanding the falling short by the controller, there is no actual risk to data subjects' rights.

279. TikTok's reliance on the EDPB Supplementary Measures Recommendations in this respect is also misplaced. It is true that the Recommendations do envisage that a controller, having *correctly identified* that there is a theoretical lack of equivalent protection could decide to make a transfer without putting in place measures to address any deficit where there is no reason to believe that there is *in fact* any risk, but only if this analysis is demonstrated and documented. TikTok appears to suggest, that where a controller *fails* to identify whether there is a lack of equivalent protection, and necessarily therefore fails to assess the risk posed by an identified lack of protection and demonstrate and document why it is nonetheless considered safe to proceed with a transfer, the DPC should have carried out the analysis that TikTok failed to before finding an infringement. That is plainly not the case.

280. In the particular circumstances of this case, somewhat different considerations arise for the purpose of considering whether a corrective order requires to be made, or an administrative fine should be imposed. Since controllers are not entitled to transfer personal data to third countries unless effectively equivalent protection is guaranteed, where a decision-maker finds that effectively equivalent protection is not guaranteed in a third country, because there is no adequate assessment which establishes the level of protection which is available, the further transfer of personal data will typically not be permitted.

281. In this regard, it is important to distinguish the position here, where the DPC found that TikTok had failed to adequately assess the level of protection available, and that at issue in *Schrems II*, where there had been such an assessment, and a conclusion that there was inadequate protection available. In those latter circumstances, as *Schrems II* makes clear, the supervising authority is obliged to suspend the transfer of data where the controller has not

already done so. In this instance, the DPC finding of infringement related to a failure of *assessment* not a failure of *protection*.

282. Of course, the *reason* that the CJEU concluded that it was necessary to suspend transfers in the scenario considered in *Schrems II* was because essentially equivalent protection could not, as required by the GDPR, be guaranteed. Where there has been a failure in assessment of the level of protection actually available, then, necessarily, equivalent protection cannot be guaranteed. In those circumstances, it would normally follow from a finding that a controller had not assessed, or adequately assessed, the level of protection in a third country that any further transfers should be suspended until an adequate assessment is completed, and equivalent protection can be guaranteed.

283. However, in this instance, the DPC elected to fix the temporal scope of the Inquiry as ending at 17 May 2023. Its finding of infringement was, accordingly, made on the basis of a different factual scenario than that which existed at the time of its decision to make the suspension order. Significant changes had been made by TikTok since that date, and detailed additional information had been provided, all of which the DPC had repeatedly stated it would have regard to for the purpose of the Inquiry. Though, as discussed below, it is difficult to see how TikTok was prejudiced by the DPC's decision in relation to the temporal scope for the purpose of the infringement finding, it would clearly have been prejudiced if the DPC did not consider that additional information in determining whether, notwithstanding the infringement finding, it was appropriate to make a suspension order.

284. The infringement finding was a finding of *historic* non-compliance. There is nothing in the GDPR or *Schrems II* which suggests that such a finding necessitates a *prospective* suspension.

285. Moreover, Recital 129 of the GDPR provides that “*each [corrective] measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation.*” That must apply with particular force in this case where the corrective measure was being imposed almost two years after the temporal scope of the Inquiry and, therefore, of the infringement finding, and where the DPC acknowledged that significant changes had been made to the manner in which the transfers took place. An automatic suspension of transfers in those circumstances would not necessarily be proportionate.

286. Although the Decision refers to *Schrems II* and the obligation to suspend where essentially equivalent protection is not guaranteed, it is plain that the DPC in fact carried out a detailed assessment of whether a suspension order was appropriate in the circumstances, as recorded in the Decision (at §682):

682. In order for 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. 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 following an infringement of Article 46 GDPR.

287. As we will see, as part of that assessment, it concluded that TikTok still had not adequately assessed the level of protection available in China. It also concluded that the other supplementary measures relied on by TikTok did not overcome this failure. The merits of those conclusions are addressed below, but TikTok has not identified any error of law in the approach taken by the DPC.

Overall conclusion on Ground 3

288. In the circumstances, Ground 3 of the grounds of appeal is rejected.

289. The DPC did not misdirect itself in law, and did not misinterpret *Schrems II*. It had appropriate regard to Article 5(1) and 24 of the GDPR when interpreting Article 46. There was no impermissible reversal of the burden of proof in making the Decision. There was no error in the Decision by reason of the DPC's failure to carry out a risk assessment. No issue of risk assessment arose in relation to its finding of infringement. It appropriately considered the proportionality of the suspension order before making it.

Grounds 1 – Breach of fair procedures

290.At Ground 1 of its appeal, TikTok alleges various breaches of fair procedures.

291.Firstly, and perhaps fundamentally, at Ground 1(a) it argues that it was not notified of the concern upon which the DPC relied to make its first finding, that TikTok had transferred data in breach of Article 46(1), and therefore it was not in a position to address it directly. This, claims TikTok, was a breach of the right of the defence, that a person must be put in a position to know the case against them and be given an opportunity to respond. It referred to a number of cases in support of this general proposition, including Case C-530/12, *OHIM v National Lottery* in which the CJEU observed (at §54):

“The rule that the parties should be heard does not merely confer on each party to proceedings the right to be apprised of the documents produced and observations made to the Court by the other party and to discuss them. It also implies a right for the parties to be apprised of the matters raised by those courts of their own motion, on which they intend basing their decision, and to discuss them. In order to satisfy the requirements relating to the right to a fair hearing, it is important for the parties to be apprised of, and to be able to debate and be heard on, the matters of fact and of law which will determine the outcome of the proceedings (Commission v Ireland and Others, paragraphs 55 and 56, and Case C-472/11 Banif Plus Bank [2013] ECR, paragraph 30).”

292.In the alternative, it argues at Ground 1(b) that it had, in fact, provided information which addressed the DPC’s concern, in particular, at footnote 113 of the July 2024 DTA, and also in the second and third Xu opinions, and that the DPC failed to have adequate regard to that information. This ground overlaps to a significant degree with Ground 2 of its appeal by which TikTok contends that the DPC made a manifest error in concluding that the issue of concern had not been addressed by TikTok. Put otherwise, TikTok claims that either the DPC disregarded relevant information (the contents of the July 2024 DTA and the Xu opinions), amounting to a breach of fair procedures, or if it did have regard to the relevant information, it erred in its understanding of it.

293. TikTok also pleads, at Ground 1(c), that the DPC erred in its assessment of the material provided by the DPC regarding Project Clover. In particular, it contends that the DPC failed to put its findings regarding Project Clover to TikTok and afford it an opportunity to address them and, in any event, failed to have adequate regard to those submissions. At Ground 10, TikTok alleges material errors in the assessment of the Project Clover information. There is a clear overlap between these grounds.

294. TikTok pleads, at Ground 1(d), that the amendment of the temporal scope of the Inquiry from “ongoing” to a scope concluding on 17 May 2023 (the date of the PDD) breached its legitimate expectation and was in breach of fair procedures. In this regard, it contends that the amendment of the temporal scope meant that the DPC did not assess, or assessed only cursorily, information provided by TikTok after the PDD, contrary to assurances to the contrary, and in any event, only considered that information insofar as it related to the question of suspension and not in relation to the infringement.

295. Finally, TikTok pleads, at Ground 1(e), that it was unlawfully denied access to the DPC’s file both during the Inquiry, when it requested the file after receipt of the Draft Decision, and again following receipt of the Decision.

296. TikTok also makes a more generalised complaint, articulated in oral submissions regarding the failure of the DPC to engage with it, in particular, its purported failure to seek clarifications, to highlight areas which had not been addressed, or to meet with TikTok, particularly having regard to the significance of the issue for TikTok. It refers to the decision in *Shatter v Guerin* [2021] 2 IR 415 (at p. 520):

“... the level of fair procedures must relate to and be a proportionate engagement (i) with the declared concerns of the decision-maker, which, if left at such level, would be published in that form and (ii), with a reasonable appreciation, objectively realised, of the imputations on character which such published concerns may give rise to.”

297. Before considering each of these alleged deficiencies in turn, it is important to recall what is stated above regarding the scope of the appeal. In principle, breaches of fair procedures are capable of being remedied by an appeal, where an appeal is available. Where a breach of fair procedures is not capable of being remedied by an appeal, then the

appropriate remedy is judicial review. Though TikTok has also issued judicial review proceedings, it has elected to pursue its statutory entitlement to appeal. It seems to me, therefore, that for the purpose of this appeal it is required to accept that the breaches of fair procedure it identifies are at least *capable* of being remedied in this appeal. In an appeal, as in this case, where an appellant is in principle entitled to adduce new evidence, the appeal mechanism must be regarded as effective to address any procedural deficiency before the DPC. I do not accept, therefore, the argument advanced in oral submissions and in its supplemental written submissions that identifying a breach of fair procedures is necessarily a basis for TikTok to succeed in its appeal. Rather the consequences of any breach must be considered in the context of the appeal as a whole.

Failure to put adverse findings to TikTok

Arguments

298. The main complaint made by TikTok under this heading is that the DPC's concerns altered dramatically between the PDD and the Draft Decision. TikTok says that it addressed the complaints identified in the PDD but was never given an opportunity to address "*new*" concerns identified for the first time in the Draft Decision. In particular, TikTok argue that the PDD identified, in paragraph 253, that "*two key concerns*" remained, and that these were set out at paragraphs 254 to 257, quoted above, and reiterated at paragraphs 368 – 371. TikTok's position is that it fully addressed those concerns, but contends that it could not have understood from the PDD that the DPC was concerned about the issue which led to its finding of infringement, the extent of protection afforded to personal data *while it was being processed in China*, which I will refer to as the "*local processing concern*" or the "*local processing issue*". TikTok argues that it was, therefore, prevented, in breach of fair procedures, from having an opportunity to meet the case being made against it. When it became aware of this new concern being relied on by the DPC, upon receipt of the Draft Decision, it sought an opportunity to address this new concern and requested that the Draft Decision be withdrawn. It supplied additional information, including the third Xu opinion, but this request was rebuffed and the new information disregarded.

299. TikTok contends that it was a requirement of EU law that the DPC provide its preliminary views to it, citing Case C-349/07, *Sopropé* at §36- 37, although that decision

says no more than that the addressee of a decision which significantly affects its interests must be put in a position where it can make known its views on the information on which the authority intends to base its decision. As the parties note, the requirement to draft preliminary findings is now included in Article 19(1) of the Procedural Regulation for GDPR Enforcement (Regulation (EU) 2025/2518). Article 19(7) provides that those under investigation shall be given an opportunity to reply. However, the parties agree that the Regulations are not applicable to this Inquiry as they will only apply from 2 April 2027 (*per* Article 37).

300. In any event, TikTok argues that the same protections apply as a matter of domestic law, citing *Shatter v Guerin* and *Zalewski v Workplace Relations Commission* [2022] 1 IR 421.

301. TikTok argued throughout the Inquiry that the DPC should issue a revised PDD where circumstances changed, or it identified new concerns, or TikTok highlighted errors in its analysis. Its pleaded case was that the DPC was under an obligation to do so, but in oral argument, it appeared to accept that there was no particular form or procedure which the DPC was required to adopt, rather what was essential was that TikTok be given an opportunity to address any issue which the DPC might rely on for the purpose of making a finding against it.

302. The DPC denies that it raised any new issue in the Draft Decision (or Decision) and says that all of its concerns had been clearly flagged in the course of the Inquiry and in the PDD. There was, accordingly, no breach of fair procedures. Though TikTok sought to adduce additional information after delivery of the Draft Decision, the DPC says it was under no obligation to consider it, having regard to the stage of the procedure at which it was delivered. In any event, it argues, the additional information, in particular the third Xu opinion, did not address the DPC's concerns.

303. As regards the requirements of fair procedures generally, the DPC highlights the observations of the court (Barniville J, as he then was) in *Facebook Ireland Ltd v DPC* [2021] IEHC 336 (at §263):

“It is clear from the GDPR and from the judgment of the CJEU in Schrems II that it is necessary for the supervisory authority to balance and attempt to reconcile the right to

be heard and to fair procedures on the part of those who are the subject of an investigation or inquiry conducted by a supervisory authority against the obligations on the supervisory authority to act within a reasonable time and with due diligence in determining whether the GDPR has been infringed and in determining what, if any, corrective powers should be exercised. That can be a difficult balance for the supervisory authority and, in this case, the DPC, to achieve, but both rights and obligations must be properly taken into account by the supervisory authority in terms of the procedures which it applies. One does not necessarily trump the other and individual assessment will be required to be made by the supervisory authority in each case.”

304. Insofar as the DPC *did* provide its preliminary findings to TikTok, it does not argue that it was free to rely on entirely new issues in reaching the Decision, but argues that its final findings were not required to “*correspond precisely*” with the provisional findings, and references Cases T-194/06, *SNIA* at §80 and T-344/17, *Latam Airlines Group* at §210 and §216. It argues that it did no more than “*develop*” the preliminary findings in response to the submissions received and that there was no significant change to the fundamental issues identified in the PDD.

305. The position in relation to the third Xu opinion is somewhat opaque. At §691 of the Decision, as referred to above, it is stated that regard was had to material submitted after the Draft Decision, including this report, but that it did not address the DPC’s concerns. In its letter of 25 March 2025, it stated that “... *even considering TikTok Ireland’s most recent correspondence in the context of the ongoing transfers, it is clear that fundamental flaws identified in the Draft Decision remain unaddressed and ongoing*” which suggests that the contents of TikTok’s correspondence, including the third Xu opinion, had been assessed, albeit the reasons for concluding that flaws remained is not set out.

306. However, the various pleas in relation to this issue in the Statement of Opposition are to the effect that the DPC was not required to have regard to that opinion, having regard to the late stage at which it was submitted. At §109.5 of the Statement of Opposition, the DPC seeks to “*contextualise*” the statement at §691 of the Decision:

While the DPC had regard to the fact that TikTok Ireland had submitted the Third Xu Opinion, in circumstances where the Third Xu Opinion was submitted three weeks after the submission by the DPC of the Draft Decision to the Article 60 Process, it is evident that the reasoning of the Draft Decision could not at that stage be altered having regard to the content of the Third Xu Opinion, and it is not contended that the content of the Third Xu Opinion is addressed in the Decision. The DPC did not consider that the Third Xu Opinion required or justified the withdrawal of the Draft Decision from the Article 60 process by reason of the timing of its receipt and for the reasons identified in the DPCs correspondence of 25 March 2025. In that respect, and for the avoidance of doubt, it is not accepted that the Third Xu Opinion addresses the DPCs concerns with respect to the application of the Relevant Chinese Laws to the Transfers or is such as to require alteration of the DPCs conclusion with respect to the corrective measures required.

307. The Statement of Opposition is verified by Mr Cian O'Brien, a deputy commissioner, who is head of the unit within the DPC which had carriage of the Inquiry. He was not, however, the decision-maker.

Discussion

308. It is, at first blush, surprising that TikTok would suggest that the DPC's identification in the Draft Decision of concern about the level of protection afforded to personal data transferred to China *while it is being processed* in China was a new issue. The fact that data was being transferred to China and processed there was, from the outset, the subject of the Inquiry. It's why there was an inquiry. More importantly, perhaps, it is the very issue which Article 46 required TikTok to address. In fact, this is true even on TikTok's narrow (and, as I have concluded, mistaken) view of the scope of Article 46. Even if TikTok was only required to satisfy itself that equivalent protection was available for personal data transferred to China, without any obligation to be able to demonstrate that this was so, it was the data actually transferred which required to be assessed.

309. To explain, the GDPR is primarily concerned with processing of personal data. This is apparent from Articles 5 and 24, discussed above. There are also, of course, rights associated

with the retention of data by controllers and processors, albeit not at issue in this appeal. Processing is defined broadly in the GDPR, in Article 4(2), set out above.

310.Article 44 concerns transfers of personal data outside the EU, but it doesn't define transfers. It applies, however, to transfers which "*are undergoing processing or are intended for processing after transfer to a third country.*" That, therefore, determines the scope of Article 46. It is concerned with data which is *actually* transferred and is undergoing processing or is to be processed in third countries. The focus of any inquiry into compliance with Article 46, on whatever view one takes of that provision, must always be on the personal data that is transferred and processed.

311.That this was so in this case was apparent from the outset. The Notice of Commencement refers to the CGE personnel "*accessing*" personal data of TikTok users in order to provide support services connected with the operation of the Platform. It states that those transfers will be the subject of the Inquiry, *i.e.* the personal data which was being accessed.

312.TikTok's reply to the Notice highlighted the storage of data outside China and significant access restrictions on those who could access the data from China. It updated its DTA as described above.

313.The DPC's second RFI raised detailed queries. It expressly asked what was the technical means by which data was remotely accessed. In response, TikTok once again referred to storage outside China, and referred back to the access restrictions described in its first response. It did not explain in any detail the technical means by which data was accessed, only the restrictions on how that data was accessed.

314.The DPC then issued a Statement of Issues in which, it stated, it was not expressing any preliminary views. In its responses and DTAs, TikTok repeated its reliance on the fact that remotely accessible data was stored outside China and therefore outside the jurisdiction of the Chinese authorities.

315.At paragraph 74 of the PDD, the DPC stated:

The concept of a “transfer to a third country” is not defined in the GDPR. However, the EDPB has clarified that both “remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is [...] considered to be a transfer.” It is clear that remote access to personal data of EEA users by personnel of the China Group Entities falls within the concept of a “transfer” for the purpose of Chapter V of the GDPR.

316. This is accepted by TikTok. It is against that background one must consider TikTok’s claim of breach of fair procedures having regard to the contents of the PDD. Insofar as the PDD raises concerns about the ability of Chinese authorities to access data stored outside China, it may be that the DPC was distracted by TikTok’s focus on the territoriality issue. Data stored outside China and *not* accessed remotely from China was not data transferred within the meaning of Chapter V (the DPC made clear that it was not concerned with any transfers other than those to China for the purpose of the Inquiry). Data stored on servers outside China does not give rise to any issue under Chapter V of the GDPR not because of the territoriality principle, but because it is not data transferred to China at all: it is outside the scope of Chapter V. The only data with which the DPC should or could have been concerned was the data actually transferred to and processed in China. This is not to suggest that no issue might arise under the GDPR where such data is *accessible*, only that no issue appears to arise under Chapter V.

317. Although TikTok repeatedly stated that the DPC’s concerns were all about storage, in truth it was TikTok who sought to make storage the issue. Where the data was stored is relevant because of TikTok’s reliance on the territoriality principle. It, however, was never the subject of the Inquiry. Rather, it was TikTok’s answer to the concerns raised.

318. Those concerns, as we have seen, were reduced to “*two key concerns*” in the PDD. TikTok characterise the two concerns as the “*extraterritorial application concern*” and the “*foreign server concern*”. In this regard, it says that the extraterritorial application concern, expressed in §254 of the PDD, was whether the relevant Chinese laws applied extra-territorially. It says that the foreign server concern, expressed in §255- 256 of the PDD, was whether, in effect, the CGEs or their employees could be compelled to provide assistance in accessing data stored outside China. As noted by TikTok in its oral submissions, this issue

of compellability was the focus of the DPC's concerns in its analysis of Issue 3 (§368 – 371 of the PDD).

319. The DPC's characterisation of the two key concerns, in its written submissions, is that the first concern related to the extraterritorial effect of the relevant Chinese laws, and, therefore, it agrees with what TikTok contends was the first concern. It rejects TikTok's characterisation of the second concern, which it states related to the application of the territoriality principle in the "*specific factual context of the Data Transfers*".

320. Neither party's characterisation reflects how the second concern was described in the Decision, which does state (at §354) it was the application of the territoriality principle in the specific factual context of the Data Transfers, but that this concern was based on two issues, first, the compellability of CGEs and their employees, and second, vagueness as to the exact contours of the territoriality principle.

321. The precise characterisation of the concerns identified in the PDD is less relevant than is the question of whether TikTok was given a fair opportunity to address all the DPC's concerns, or whether, as it alleges, the findings in the Decision were based on new findings and concerns not put to TikTok.

322. The specific objection made by TikTok is set out at paragraph 45 of its written submissions. It says that the DPC "*introduced new findings*" that remote access results in EEA User data being processed on computer systems in China as an "*inevitable consequence of any remote access solution*" and that "*arising from this*", the Draft Decision introduced a new adverse finding, what it calls the "*temporary processing finding*", that TikTok had not addressed the application of the relevant Chinese laws to the processing which occurs on computer information systems in China. It contends that this conclusion was relied on for the purpose of additional adverse findings. It argues that in breach of fair procedures, it was not given an opportunity to address this concern.

323. Given the emphasis placed by TikTok on the unfairness of the DPC's reliance on this "new" finding, it is important to emphasise that TikTok does not dispute the factual basis underpinning that finding. In fact, in its 11 March 2024 response to the DPC's fourth RFI, it states:

[The] transitory processing of data is an inevitable consequence of any remote access solution in order for the data to be available to be displayed to, and used by, the relevant user on its device. Without this local transitory processing, remote access would not be possible.

324.It made the same point in its first letter replying to the Draft Decision in which it contended that the DPC had erred in concluding that the local processing issue had not been addressed. Indeed, one of the errors of assessment claimed by TikTok in the appeal is that the DPC failed to take into account that transient processing was inherent to the facilitation of remote access (see §96(c) of TikTok’s written submissions).

325.Moreover, as I have indicated above, the processing of the personal data in China was *necessarily* the subject matter of any inquiry into compliance with Article 46. In those circumstances, it ought to have been no surprise to TikTok that that was the issue which it was required to address in the Inquiry. TikTok’s complaint, in effect, is that it was led to believe by the PDD that the *only* issues with which the DPC remained concerned were those identified in the PDD as characterised by it, that the processing of data in China was not one of those concerns, and that it was a breach of fair procedures for the DPC to rely on different concerns to those identified in the PDD to ground a finding of infringement of the GDPR.

326.I agree with TikTok that, in line with the principles identified in the EU and domestic case law relied on by it, and the rights of the defence, that it would have been a breach of fair procedures for the DPC to rely on issues which were not put to TikTok when making findings that TikTok had breached the GDPR. I do not, however, agree that this is what occurred here.

327.The processing of the data in China was at all times the subject of the Inquiry and at all times required to be addressed by TikTok. There is nothing in the PDD which could have led TikTok to believe that no concerns remained regarding whether effectively equivalent protection was guaranteed in relation to personal data being processed in China. While this portion of the judgment is concerned with the allegation of breach of fair procedures, we will see, when considering Ground 2 of the appeal, I agree with the DPC’s conclusion that

TikTok had not addressed this issue at the time of the PDD (or indeed at any time prior to its submission of the third Xu opinion).

328. To step back for a moment, TikTok's thesis is that the data accessed in China is stored in data centres outside China, and that Chinese authorities have no jurisdiction to compel access to data which is stored outside China. TikTok has treated this as a full answer to the question of whether data *actually being processed* in China was also outside the jurisdiction of Chinese authorities. It manifestly is not. The fact that Chinese authorities cannot access data stored overseas, because it is stored overseas, without more, tells us little or nothing about whether Chinese authorities can access data being processed in China. At the absolute minimum, it would have been necessary for TikTok to show that there is nothing *capable* of being accessed in China, notwithstanding the wholesale processing of data there by CGE employees, or that *as a matter of Chinese law* data processed on computers in China but permanently stored overseas is itself treated as overseas data. As we will see, TikTok never asserted the former. The first time that anything like the latter was suggested was in the third Xu opinion.

329. The distinction between where data was stored and where it was processed was highlighted to TikTok in the second RFI, literally, since the words 'stored' and 'processed' were underlined in Query V(3). TikTok's response said nothing about data processed in China, only data stored outside China.

330. TikTok's position, since it accepts that it was implicit that data was being processed on computers in China, is that Chinese authorities would, in effect, accept that they could not access data being processed in China under any of the relevant Chinese laws because it was permanently stored overseas. The basis for that proposition was not explained. In any event, it was the issue which was at the heart of the Inquiry and the DPC had made clear that it had not been addressed by the time it delivered the second RFI. Since TikTok's response to that RFI, and in particular, queries about the technical means of accessing data and the processing in China ignored the underlying premise of those questions, the fact of the matter is that it had not been addressed by the time of the PDD.

331. Far from providing comfort to TikTok that this central issue had been adequately addressed, a fair reading of §254 to §257 of the PDD makes clear that those concerns

remained. §254 identifies that the DPC was not satisfied that the relevant Chinese laws did not apply in the specific factual context of the transfers. The first concern articulated in §254 assumes that TikTok's explanation of the territoriality principle is accurate but seeks clarity on those laws which may, in fact, have extra-territorial effect. The second concern makes clear that the DPC is not convinced that reliance on the territoriality principle is an answer:

The second concern relates to the basis for the premise that TikTok Ireland's analysis regarding the application of the territoriality principle in the specific factual context of the transfers is accurate. The concern itself is that TikTok Ireland has furnished insufficient information in the Inquiry to enable me to conclude that the territoriality principle does in fact operate so as to prevent the application of problematic surveillance laws, such as the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law and National Intelligence Law, to the personal data of EEA users the subject of the transfers, save in situations where those laws have extra-territorial effect.

332. Put in simple terms, TikTok has not explained why the relevant Chinese laws would need to have extra-territorial effect in order to be applied “*in the specific factual context of the transfers*” to the “*personal data of EEA users the subject of the transfers*”. Why, in other words, do these laws not apply to the personal data being processed in China?

333. It identifies in the following paragraphs reasons why it wasn't satisfied (primarily, the compellability of CGEs and their employees). At §257, the PDD specifically concludes that TikTok has been vague about the exact contours of the territoriality principle. In this regard, it will be recalled that at that stage of the procedure, TikTok's main basis for contending compliance with Article 46 was the storage of data outside China and its interpretation of the territoriality principle. The PDD went on to identify that TikTok had not identified legal authorities which interpret the principle in the manner they contend for:

... in practice in a scenario that is analogous to the present one, concerning remote access, using technical means, by persons within the jurisdiction of China to data stored on servers in a foreign jurisdiction.

334. TikTok had every opportunity to adequately address the precise scenario described here. At the hearing of the action, I expressly enquired of TikTok why this wasn't sufficient to put it on notice regarding the issue which ultimately formed the basis of the DPC's infringement finding and it was suggested that in these paragraphs of the PDD, the DPC was talking about "*accessing the data in the servers*" (Transcript, Day 1, p. 25). That may be so, but the statement at §257 clearly identifies that the concern is with the access by technical means *within* China.

335. If there were any doubt regarding whether the DPC was concerned with what was actually happening in China, the fourth RFI put it up in lights, highlighting that, insofar as TikTok relied on where data was *stored* as an answer to any concerns regarding the level of protection for transferred data, TikTok had not explained how it is that they contended that data being processed in China was not stored there. TikTok seeks to suggest that a request for further information after the PDD was unusual and, at least implicitly, criticise the DPC for raising this query (Transcript, Day 1, p. 21 and p. 87). Its position in this regard is wholly inconsistent with its claim of its breach of fair procedures and that the DPC should have issued a revised PDD. Having considered TikTok's response to the PDD, it was entirely appropriate for the DPC to have sought clarification on what TikTok was saying. It certainly provided TikTok with a further opportunity to explain how its remote access solution ensured essentially equivalent protection for data being processed in China.

336. TikTok's response is enlightening for what it does and does not contain. It does contain TikTok's opinion that there is no storage in China, by reference to Oxford English Dictionary and Collins Dictionary definitions of the word "storage". The OED definition it provides is "*the action of storing or laying up in reserve*" or store "*a stock of anything... laid up for future use*". It is curious that it did not use the definition provided by the OED relating to computing "*the retention of retrievable data on a computer or other relevant electronic system*", but the more relevant issue is that it is difficult to see what possible relevance an OED definition could have to the question of whether, *as a matter of Chinese law*, data processed in China by remote access is not regarded as stored there. What is missing from the response, of course, is any Chinese law analysis of whether the data processed in China would be regarded as stored there, still less, any Chinese law analysis which suggests that the relevant Chinese law could not be applied to the data being processed in China.

337. TikTok seek to compare the language in the Decision where it is concluded that the issue of processing of EEA user data on computer information systems in China hadn't been addressed, with the language used in the PDD to suggest that the Decision was addressed to issues not raised in the PDD. I do not agree. When one understands that the focus of the Inquiry was always data transferred to China, when it is accepted by all that processing on computer systems in China is an inevitable consequence of the remote access solution, the issues of concern identified in the PDD, and the subsequent RFI gave TikTok a more than adequate opportunity to address the issue which ultimately led to the first finding of infringement. If TikTok failed to do so, which I will consider when we turn to Ground 2, it was not due to any lack of fair procedures.

338. Particularly when considered in context, there was no lack of fair procedures in the procedure adopted by the DPC. This complaint does not provide any basis for interfering with the DPC's conclusion that there had been an infringement of Article 46 by TikTok.

Failure to have regard to submissions made

Arguments

339. TikTok's alternative argument is that even though it was not aware that the processing of personal data in China remained one of the DPC's concerns, it did, in fact, address the level of protection afforded to such processing, in the July 2024 DTA, at footnote 113, and again in the third Xu opinion, provided after the Draft Decision. It suggests that it had also *implicitly* addressed the issue in the second Xu opinion, and that this was expressly confirmed in his later opinion.

340. The Decision is silent on footnote 113. Insofar as the claim in relation to footnote 113 is a fair procedures claim, it is a claim that the DPC failed to have regard to relevant information or failed to engage with relevant information. TikTok refers to *Balz v An Bord Pleanála* [2023] 3 IR 751 in its submissions to the effect that decision makers must address relevant submissions and provide explanations for why they are not accepted. In fact, TikTok has not pleaded a claim that the DPC failed to provide reasons for its 'rejection' of footnote 113 as an answer to the concerns raised in the PDD. The DPC says in response that it was only required to engage with "*significant submissions*", citing *NECI v Labour Court* [2022]

3 IR 515. It argues that footnote 113 does not address its concerns regarding the application of the territoriality principle to the data transferred to China and in its written and oral submissions explains why this is so.

341. The position in relation to the third Xu opinion is different. The Decision *does* reference the opinion, though only for the purpose of saying it didn't address the concerns identified in the Draft Decision. It appeared, therefore, that the DPC had had regard to that submission, but its formal position now, in response to the fair procedures claim, is that it did not address it in the Decision, nor was it required to because it came so late in the day. In this regard, the DPC argues that by the time the third Xu opinion was submitted, "*the opportunity for further comment must legitimately be considered to have ceased in all the circumstances*" (DPC legal submissions at §64).

342. In this regard, the DPC refers to the decision in *The State (Haverty) v An Bord Pleanála* [1987] IR 485, highlighting the emphasis placed by the court in that case on achieving finality in proceedings. In that case, a successful objector to a development before a planning authority was not provided with an opportunity to comment on additional submissions submitted by the developer in its appeal against the planning authority's refusal. Though the DPC is correct as to the court's conclusion, the full analysis is worth setting out (at pp. 493/494):

"The essence of natural justice is that it requires the application of broad principles of commonsense and fair play to a given set of circumstances in which a person is acting judicially. What will be required must vary with the circumstances of the case. At one end of the spectrum it will be sufficient to afford a party the right to make informal observations and at the other constitutional justice may dictate that a party concerned should have the right to be provided with legal aid and to cross-examine witnesses supporting the case against him. I have no doubt that on an appeal to the planning board the rights of an objector — as distinct from a developer exercising property rights — the requirements of natural justice fall within the former rather than the latter range of the spectrum. This flows from the nature of the interest which is being protected, the number of possible objectors, the nature of the function exercised by the planning board and the limited criteria by which appeals are required to be judged and the practical fact that in any proceedings whether oral or otherwise there must be finality. Some

party must have the last word. The substantive reality of the present case is that the prosecutrix and the Sefton residents' association put forward a detailed professional argument before the planning authority in the first instance and the planning board in relation to the appeal. I can appreciate their concern that they might have wished to expand upon their argument or to raise counter-arguments to those made in reply by the developers but I have no doubt that the real substance of their case was before An Bord Pleanála and duly considered by it. If there was in fact a material conflict of evidence that could not have been resolved by additional submissions or observations. Disputes of that nature could only be adequately dealt with in an oral hearing.

To avoid misunderstandings perhaps I should make it clear that I do not accept and I have not accepted any general proposition that An Bord Pleanála could discharge its obligation to an interested party by delivering part only of the appellant's submission to any person entitled to receive the same. I could imagine cases in which further communications from the developer extended the original submission so radically as to constitute a different or additional case and in that event natural justice might well require An Bord Pleanála to postpone its decision until it had afforded interested parties an opportunity of commenting upon the revised submission. However, as I say, in the present case it seems to me that whilst the prosecutrix and her planning adviser do feel strongly that they would wish to have had an opportunity of amplifying the arguments which they had made I believe that the requirements of natural justice have been met so that there are no grounds for granting the order sought. I would allow the cause shown with no order as to costs.”

343. The DPC also refer to the decision in *Klohn v An Bord Pleanála* [2009] 1 IR 59 to similar effect, and to the decision of Barniville J in *Facebook Ireland v DPC*, referred to above, regarding the necessity to balance the right to be heard with the obligation on a supervising authority to act within a reasonable time and with due diligence.

Discussion

344. There is no real dispute between the parties regarding the legal obligation to have regard to submissions made: there is, of course, no inconsistency between *Balz* and *NECI*. *Balz* makes clear that it is necessary “*that relevant submissions should be addressed and an explanation given why they are not accepted*”. In *NECI*, MacMenamin J refers to *Balz* as making clear that “*a decision-maker must engage with significant submissions*”.

345. In relation to footnote 113, the question of whether there was any breach of fair procedures by the DPC in failing to refer to it largely depends, therefore, on whether it does in fact address the issues raised in the PDD and which led to the findings of infringement, an issue addressed when considering Ground 2, in other words whether it was relevant to that issue. It is clear that it was not considered of sufficient relevance by the DPC to warrant being addressed in its decision. The DPC is correct insofar as it says that the fact that it is not referred to does not establish that it was not considered. TikTok submitted thousands of pages of documents to the DPC. Necessarily, not all of that material is referred to in the Decision. This does not mean that it was disregarded.

346. Footnote 113 is contained in a document which was not prepared as a response to the PDD or indeed for the purpose of the Inquiry at all, the July 2024 DTA, although the covering letter enclosing that DTA noted that TikTok expected that the DPC would wish to have regard to it for the purpose of the Inquiry. It was contained in a portion of that document ostensibly addressing a different issue than the local processing issue. Also, and obviously, it is contained in a footnote, hardly the place where one might expect TikTok to provide an answer to the DPC’s continuing concerns. Of course, since TikTok claim to have been unaware of those concerns, it is, in effect, only by chance that TikTok purports to have addressed them at all.

347. TikTok’s covering letter highlighted what it considered to be the “*material*” changes between the July 2024 DTA and the previous DTA. It did not suggest that there was any significance to the addition of footnote 113, which was a note added to identical text contained within the previous DTA. Accordingly, the DPC cannot be criticised unduly for failing to expressly address footnote 113 even if it does prove to have been significant. Be that as it may, where it is not addressed at all, I do not think that the court should defer to

the DPC's assessment of it for the purpose of this appeal, whether as to its significance or its substance, rather it must be assessed solely on its merits. Its significance, or otherwise, is addressed at Ground 2.

348. It is a little more difficult to understand why the third Xu opinion was not addressed, or, for present purposes, why the DPC consider that there was no requirement to address it. I accept that it came late in the day, but the DPC had made a rod for its own back by reassuring TikTok that it would have regard to all information submitted. Moreover, the consultation period with the SACs was still open, and the DPC has not argued that there was a legal impediment to it considering the new information, whether the consultation period remained open or not. Indeed, it expressly accepts that draft decisions may be withdrawn from the Article 60 process (DPC legal submissions at §61).

349. In circumstances where the obligation on TikTok was to confirm that equivalent levels of protection were guaranteed in *advance* of transferring data, it would have been entirely reasonable for the DPC to fix a point beyond which further material would not be accepted. *Haverty, Klohn* and *Facebook* certainly suggest that they would have been so entitled. There was certainly no general obligation on the DPC to have regard to a continuous stream of information provided by TikTok for the purpose of addressing something which was required to have been addressed before any transfer of data was made. However, the DPC did not stipulate an end to the submission phase of its Inquiry, rather it assured TikTok that it would consider any new material submitted. The fact that it had issued the Draft Decision and circulated it pursuant to Article 60 may have led to an understandable reluctance by it to consider new material or re-consider the Draft Decision, but this alone could not justify a refusal to do so.

350. What is more, the DPC *did* consider material submitted by TikTok *after* the third Xu Opinion, regarding its audited accounts for the purpose of calculating the fine, and, more relevantly, regarding updates to Project Clover (see §691 of the Decision). When asked to explain why it had regard to the Project Clover material but not the third Xu opinion, counsel for the DPC offered the suggestion that the third Xu opinion was more relevant to the question of whether there was an infringement, whereas the Project Clover measures were relevant to the question of whether to make a suspension order (Transcript Day 7, pp. 22 – 24). It is not clear that this is so. It may have been the Project Clover measures were not

relevant to the infringement finding, but the third Xu opinion was clearly potentially relevant to the question of whether the suspension order should be made.

351. *Haverty* suggests a common-sense approach to fair procedures. In the circumstances of a planning appeal, where the rights of an objector were at the lower end of the spectrum of rights engaged, there was no breach of fair procedures in not affording that objector a further right to be heard. The interests of TikTok in the Inquiry are clearly at a different end of the spectrum to that of the objector in *Haverty*. Moreover, the DPC had indicated that it would consider further information received from TikTok and, critically, *did* consider information received after the third Xu opinion. Its explanation for so doing was unconvincing since the third Xu opinion was, at least potentially, as relevant to the proposed suspension order as were the Project Clover updates. There must be some obligation on a decision-maker to act consistently in such matters. Although the determination of when to bring an end to an investigation clearly falls within the discretion of a decision-maker, it is doubtful whether, consistent with its obligation to act fairly, it can determine that the time for submission of *some* material has passed, but at the same time have regard to other material, though submitted later.

352. In the particular circumstances of the third Xu opinion, the DPC ought, when having regard to whether to make the supervision order, and consistently with its treatment of the Project Clover updates, have engaged with the third Xu opinion for the purpose of determining, at least, whether it added anything material to what had previously been furnished.

353. The DPC's letter of 25 March 2025 appears to suggest that the DPC considered that the contents of the third Xu opinion did not address its concerns. However, it did not provide any explanation for that view. If the DPC is correct, that the third Xu opinion adds nothing to what had been submitted previously, then, as with footnote 113, it is difficult to see what complaint TikTok might have in this appeal. However, if its contents are material, it will be necessary to consider what the consequences may be for the Decision. I will, accordingly, consider the opinion when considering Ground 2, the alleged errors made by the DPC.

354. Before considering the next ground concerning the treatment of Project Clover, it is important to observe the following. The infringement finding of the DPC is confined to a

finding that the DPC had infringed Article 46 during the temporal scope, *i.e.*, up to 17 May 2023. The grounds of challenge in relation to that will be addressed presently. But insofar as TikTok rely on measures put in place *after* that date, TikTok faces an obvious challenge in relying on that material to show that there had been no breach prior to that date. That that is so in relation to the Project Clover measures is obvious, as these measures were not in place prior to May 2023 (or at least there is no evidence that they were), and was accepted by TikTok in oral submission (Transcript Day 1, p. 97).

355. But it is also the case with the material contained in the July 2024 DTA and the third Xu opinion. Even if they describe the legal position which pertained earlier than May 2023 (and, as we will see, at least in the case of the third Xu opinion, it is not clear that this is so), even on TikTok's case, its obligation was to verify *prior* to transfer. If its own DTA and legal opinions did not contain the material upon which TikTok now relies to say that it did verify, then it is difficult to see how TikTok could contend that there had been no infringement prior to its own verification, though they may, of course, be relevant to the determination of what consequences flow from such a finding of infringement. I will return to this point when addressing Ground 2.

Failure to adequately assess Project Clover

Arguments

356. TikTok's fair procedures complaint in relation to Project Clover is in two parts. First, it contends that the DPC did not adequately assess the material with which it was provided. And second, it contends that the DPC should have put its provisional findings in relation to the material to TikTok and afforded it an opportunity to respond.

357. The DPC says that it addressed the new measures introduced post-PDD in detail and points to the lengthy discussion of same in the Decision. As regards the necessity to afford TikTok an opportunity to respond, it contends that such an obligation would lead to a never-ending process, and refers to the decision in *IDA v Information Commissioner* [2024] IEHC 649 at §123:

*“Likewise, in his judgment in *McMonagail agus a Mhic Teoranta v. Ireland & A.G.*, Ferriter J. rejected the complaint made in that case on the basis that it came very close to arguing for a right to a draft adverse decision with a right to make submissions on such draft, notwithstanding that an earlier opportunity had been afforded to make submissions, a proposition for which no Irish authority had been cited. Ferriter J. observed that relevant context for the fair procedures question arising was the fact that where a planning decision involving a quarry is concerned, the applicant must be taken to know that the authorities are likely to have regard to publicly available maps and photos when assessing issues of quarry use. In rejecting a fair procedures complaint in that case, Ferriter J. attached importance to the fact that the material relied upon without specific notice was publicly available material which could have been obtained by the applicant. It was also material which could reasonably be envisaged as potentially being relied upon in the decision-making process.”*

Discussion

358. I do not consider that there was any breach of fair procedures by the DPC in its assessment of the Project Clover measures. Although, I have concluded above that in the particular circumstances of the Inquiry, the DPC ought to have at least considered the third Xu opinion, this does not equate to the far more expansive entitlement for which TikTok now contends.

359. The case law relied on by TikTok, both EU and domestic, establishes that it was entitled to know the case against it and be afforded an opportunity to respond. The PDD afforded TikTok that opportunity and it was entitled to respond. As part of that response, TikTok indicated that it was introducing additional measures to address the underlying concern of the Inquiry. There is simply no logic to TikTok’s contention that the DPC was obliged to give it a preliminary view of those measures, relied on in response to the PDD, before reaching a decision in the Inquiry.

360. First, and obviously, the Project Clover measures were introduced after transfers had taken place and, indeed, it appears after the temporal scope of the Inquiry had ended. They were first referenced in March 2023 and the first evidence of any implementation of those

measures was from September 2023. The measures, therefore, could have no relevance to the question of whether TikTok had infringed Article 46 during the temporal scope, only to the question of whether to make a suspension order or impose an administrative fine.

361. Moreover, the DPC had indicated in the PDD that it proposed making a suspension order. TikTok relied on the Project Clover measures to seek to argue that a suspension order was not warranted. TikTok had its opportunity to respond to the PDD and it did so by relying, *inter alia*, on the new Project Clover measures. By introducing new measures in response to the DPC's proposed suspension order, TikTok cannot have created an obligation on the DPC to give its preliminary views on those measures and, furthermore, an opportunity for TikTok to respond to that. It is plain that this would have the potential to lead to a never-ending process, as contended for by the DPC. The entitlement contended for by TikTok is not supported by any authority, and I reject the suggestion that there was any unfairness in the DPC not providing its preliminary views on the Project Clover measures prior to finalising its decision.

362. Nor do I think that there is substance to TikTok's contention that the DPC did not have regard to the Project Clover material.

363. The DPC made clear that it would look at additional material which TikTok supplied. There is no question, therefore, but that the DPC was under a duty to have regard to that material. The question is whether it gave the material adequate consideration. The additional material submitted by TikTok is described in detail in the Decision, at §617 – 644. At §683 – 691, the DPC sets out the reasons for its conclusions that the additional measures introduced after the PDD do not demonstrate that the data transferred to China is subject to essentially equivalent protection to that guaranteed within the EU.

364. Though TikTok disputes the merits of the DPC's assessment, it cannot be said that the DPC has not assessed the information. However, as discussed below in more detail at Ground 10, I am concerned that the *reasons* for the DPC's conclusion, in particular in relation to the pseudonymisation and privacy measures employed by TikTok are not adequately set out. In this regard, TikTok complains about the conclusion at §690 of the Decision:

TikTok Ireland has implemented privacy enhancing technologies that mean that the main identifiers associated with EEA User Data subject to the remote access are encrypted or redacted. This enables those employees to carry out work associated with EEA User Data without having sight of those identifiers. However, following Project Clover, the EEA User Data subject to the Data Transfers still constitutes personal data as defined in Article 4 GDPR because the data in question can relate to an identifiable person directly or indirectly. In particular, as set out above, the categories of data that are not encrypted or redacted include personal data such as user generated content. Furthermore, the DPC notes that pseudonymised personal data still constitutes personal data after said pseudonymisation if that data combined with additional information can identify a data subject. TikTok Ireland has not demonstrated that the EEA User Data subject to the transfers cannot be directly or indirectly linked to those data subjects, whether using that data alone or whether in combination with other personal data.

365. As discussed below, the DPC appears to be correct in concluding in the second last sentence that pseudonymised data still constitutes personal data if a data subject is identifiable. Moreover, I have no doubt that the DPC was entitled *in principle* to reach a conclusion that TikTok had not demonstrated that data subjects would not be identifiable. Such a conclusion would clearly fall within the DPC's technical expertise and be entitled to deference. However, the DPC has given *no* explanation of why it reached that conclusion. In the circumstances, it is difficult to see how the court could defer to the DPC's expertise on this issue. As we will see, having regard to the very significant complexity of the information submitted by TikTok in relation to its privacy solution, the failure by the DPC to give reasons for its conclusions on this issue gives rise to significant difficulties for the court in resolving this appeal.

Impermissible amendment of temporal scope

Arguments

366. The allegation that the amendment of the temporal scope was prejudicial to TikTok is closely related to the complaint about the assessment of Project Clover. The prejudice identified is that by fixing of the temporal scope at a date before the additional

supplementary measures were introduced, those measures were only assessed as relevant to the suspension order, not the finding of infringement. In addition, they were not assessed comprehensively, and TikTok was deprived of an opportunity to be provided with the DPC's preliminary views on those measures.

367. The DPC argue that limiting the scope of any finding of infringement could not have prejudiced TikTok and that all material was dealt with appropriately.

Discussion

368. The reason that the DPC elected to define the temporal scope in the way that it did in the Draft Decision and Decision has not been explained. It may have been a belated attempt to address the somewhat open-ended nature of the Inquiry it had allowed to evolve by undertaking to TikTok that it would consider all material submitted by TikTok.

369. Whatever the reason, it seems to me that TikTok's allegation that it has been prejudiced thereby would only have substance if there were substance to its other complaints about the assessment of material submitted by TikTok after the PDD. It cannot have been prejudiced by the DPC's failure to consider additional measures put in place by TikTok when concluding that there had been an infringement up to a date prior to the introduction of those measures. Insofar as TikTok asserts that the change in the temporal scope led to the material being disregarded, I do not see any evidence of that. I have already concluded that fair procedures did not require that TikTok be given an opportunity to respond to the DPC's assessment of TikTok's response to the DPC's preliminary findings. It is true that the information provided by TikTok in its response (and afterwards) was substantial, but the fact that TikTok put in place additional measures *after* it started transferring data to China cannot create an entitlement to an additional layer of fair procedures.

370. As noted above, I will consider the merits of the DPC's assessment of the measures introduced after the PDD when considering ground 10 of the appeal.

Failure to make the file available

Arguments

371. Following the receipt of the Draft Decision, TikTok made a number of requests for a “*complete copy of the DPC’s file*”. In particular, it looked for copies of the exchanges between the DPC and SACs which were referred to in the DPC’s correspondence enclosing the observations of the SACs. The DPC replied to the effect that TikTok had been furnished with all that it was entitled to, and that it was not obliged to provide details of its engagements with the SACs.

372. TikTok has not identified or suggested that there is anything with which it has not been provided other than any exchanges between the DPC and SACs post-Draft Decision. It argues, nonetheless, that it was entitled to this material and that the DPC’s failure to provide it undermines the Decision and has undermined its appeal.

373. It refers to Case C-358/16, *UBS Europe and Ors*, a case concerning a refusal by the Luxembourg financial supervisory authority (CSSF), to provide an individual with documents relating to the decision requiring him to resign from positions as director of bodies supervised by CSSF. The CJEU noted (at §67 – 68):

“As for the documents that must be included in the investigation file, it must be noted that it is also apparent from the Court’s case-law that although it cannot be solely for the authority who notifies any objections and adopts the decision imposing a penalty to determine the documents of use in the defence of the person concerned, it is however allowed to exclude from the administrative procedure evidence which has no relation to the allegations of fact and of law in the statement of objections and which therefore has no relevance to the investigation (see, to that effect, judgments of 7 January 2004, Aalborg Portland and Others v Commission, C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P, EU:C:2004:6, paragraph 126 and the case-law cited).

It follows from the foregoing considerations that the right to disclosure of the documents relevant to the defence is not unlimited and unfettered. On the contrary, as observed by

the Advocate General in essence in point 90 of her Opinion, the protection of the confidentiality of the information covered by the obligation of professional secrecy on the competent authorities in accordance with Article 54(1) of Directive 2004/39 must be guaranteed and implemented in such a way as to reconcile it with the rights of the defence.”

374. The Court identified what was required in the event of a conflict between interests (at §69):

“Accordingly, in the event of a conflict of, on the one hand, the interest of the person who is the subject of a measure adversely affecting him in having access to the information necessary for him to be in a position to exercise fully his rights of defence and, on the other hand, the interests in connection with maintaining the confidentiality of the information covered by the obligation of professional secrecy, it is for the competent authorities or courts to seek to strike a balance between these opposing interests in the light of the circumstances of each case (see, to that effect, judgment of 14 February 2008, Varec, C-450/06, EU:C:2008:91, paragraphs 51 and 52 and the case-law cited.”

375. TikTok also refer to the decision in Case C-109/10P, *Solvay SA v European Commission*, concerning access to the Commission’s file in a competition investigation. In its judgment in that case, the court noted (at §55):

“Infringement of the right of access to the Commission’s file during the procedure prior to adoption of a decision can, in principle, cause the decision to be annulled if the rights of defence of the undertaking concerned have been infringed (Limburgse Vinyl Maatschappij and Others v Commission, paragraph 317).”

376. Accordingly, argues TikTok, the failure to provide it with the exchanges between the DPC and the SACs undermined its rights of defence and, therefore, vitiates the Decision.

377. The DPC contends that TikTok had no entitlement to any documents other than those with which it has been provided and that it was entitled to refuse access to the exchanges

between it and the SACs as it is entitled to engage confidentially with the SACs under its duty of sincere co-operation. An obligation to disclose those details would undermine the integrity of the Article 60 process. It stresses that *UBS* and *Solvay* indicate that an entitlement to access to the file is not absolute and that *UBS* identifies that internal documents of the authority and other confidential material can legitimately be withheld.

378. In oral argument, the DPC traversed the material from the SACs which *was* provided in detail and highlighted the limited nature of the exchanges which had taken place with other SACs which had not been included in the file.

Discussion

379. As noted during the hearing, there does not appear to be any basis upon which a refusal to provide access to the file *after* a decision is made could, of itself, undermine a decision. The file may be necessary for the purpose of advancing some aspect of legal proceedings challenging a decision, but that is a matter for those proceedings. TikTok did not seek discovery of any documents the subject of this complaint.

380. Having regard to the nature of the documents which were “withheld”, I do not think that TikTok has established any entitlement to such documents. It appears to me that they fall within the type of document which the case law identifies does not require to be made available. The engagement with SACs comes at a stage in the process when those the subject of complaint could legitimately be excluded from further comment, at least where the engagement does not necessitate any material amendment to the draft decision. The LSA and SACs must be able to engage freely regarding the terms of a draft decision with a view to reaching an agreed position, as envisaged by Article 60. That engagement would be undermined if every aspect of that engagement was required to be made accessible.

381. Of course, any submissions made to which regard is had by the supervising authority must be made available. It is clear that that occurred here. TikTok has not succeeded in establishing any error by the DPC in how it made material available.

382. Even if I am wrong about that, TikTok would not be entitled to any remedy on this ground. Although *Solvay* and *UBS* both identify that a refusal to provide access to a file

could have a bearing on the validity of a decision, it is clear that this is only where the rights of the defence have *in fact* been infringed. In truth, TikTok advanced no argument that its rights *could* have been infringed by the refusal to provide material which it refused. It did not engage with what was not made available at all, rather asked the court to intervene on the basis of hypothetical or notional harm. In fact, it is almost impossible to imagine that anything which was not disclosed could have had any bearing on TikTok's rights. TikTok was provided with full copies of the SACs observations. There were no reasoned objections from any SAC. There were no material amendments to the Draft Decision in light of observations received. There was, accordingly, a vanishingly small possibility of there being anything material in any documentation withheld.

383. Had TikTok wished to assert its entitlements to the documents and then to show an infringement of its rights of defence, it should have sought discovery of the documents. If it was concluded that they were not entitled to them, then that would have been an end of the matter. Had it been found to have been entitled to them, it could then have argued by reference to those documents that its rights had been infringed. What it is not entitled to do so is ask the court to hypothesise that its rights might have been infringed by reference to documents which are not before the court and which *prima facie* could have no bearing on its rights of defence.

Ground not pleaded

384. In addition to the issues pleaded above, TikTok advanced an additional complaint at the hearing of the action that the DPC had not followed the procedure it had indicated it would follow in the Notice of Commencement. In that regard, as pointed out by TikTok at the hearing, the Notice of Commencement had indicated that the DPC would prepare a draft decision for the purpose of the Article 60 process which would be furnished to TikTok "*for its consideration and submissions before it is submitted to the Article 60 process*".

385. Leaving aside that this complaint was not pleaded, the procedure followed by the DPC in substance afforded TikTok the opportunity it said it would, to respond to the DPC's provisional findings. I note, in addition, that in its letter of 21 June 2024, the DPC advised TikTok that it would provide it with a copy of a draft decision *after* it had been circulated

via the Article 60 process. TikTok raised no objection. The complaint, therefore, is without substance.

Overall conclusion on Ground 1

386. For the reasons set out above, most of TikTok’s complaints of breach of fair procedures are rejected. However, I consider that the DPC erred in refusing to have regard to the third Xu opinion, and in concluding that Project Clover measures were not sufficient to justify not making a suspension order without explaining the basis for that conclusion.

387. As explained above, in judicial review proceedings, the possible consequence of these failures would be that the decision to impose the suspension order would be quashed, and that aspect of the Decision remitted to the DPC for further consideration. However, in an appeal on the record, I consider that the court’s task is to consider whether it is possible to remedy the DPC’s errors by assessing the information to which sufficient regard was not had, or the failure to explain the DPC’s conclusions. I will, accordingly, now consider these issues together to try and determine whether, in fact, any error occurred in the DPC’s conclusions.

Grounds 2 and 10

Alleged errors in assessment

388. As noted above, there is a significant overlap between Ground 2 and Grounds 1(a) and (b). It is TikTok’s position that it *had* assessed transient processing and that the DPC erred in concluding that it had not. As noted in its submissions (at §98), this “*error subtends all the findings of infringement of Article 46*”. Although TikTok’s ground of appeal refers to a “*manifest error of assessment*” by the DPC, in light of the conclusions in *LinkedIn* regarding the scope of an appeal under section 150 of the 2018 Act, TikTok is now essentially inviting this court to conclude that it *had* assessed the transient processing of data such that there was no failure by it to assess whether the personal data transferred was subject to equivalent

levels of protection, or, at least, on the evidence, that the DPC erred in concluding that it had not.

389.Ground 2 is concerned with purported errors in the assessment of the evidence regarding the application of the territoriality principle to the transferred data. Ground 10 alleges errors in the assessment of the Project Clover measures.

390.In arguing that the DPC has erred in its assessment of the evidence regarding the application of the relevant Chinese laws, TikTok points to three pieces of evidence which, it contends, show that it assessed the local processing issue which ultimately led to the finding of infringement against it. In this regard, it is important to recall that the obligation under Article 46, even on TikTok's analysis, is to verify the position in the third country to which data is transferred *prior* to transferring the data. TikTok point to no assessment by it of the local processing issue prior to 17 May 2023. The information it now relies on is information submitted during the Inquiry (though not all directly in response to the Inquiry). It has not sought to adduce additional evidence for the purpose of showing that the local processing issue had been addressed by it prior to transfers taking place, or at any point earlier than the submission of its response to the PDD in September 2023. On the basis of the evidence before the court, therefore, the matters relied on by TikTok are incapable of showing that the DPC erred in concluding that as of 17 May 2023, TikTok had failed to address the local processing issue. I accept, however, that the material could be relevant to the assessment of whether an infringement finding was warranted, or, whether there was a basis for imposing an administrative fine, *e.g.* if the evidence showed that there was equivalent protection in the third country, or that any failure of assessment was insignificant. This possibility appears to have been acknowledged by the DPC in the Decision (at 127):

The DPC has had regard to all relevant changes for the purposes of this Decision. While the temporal scope of the Inquiry ends on 17 May 2023, the DPC has had regard to all information submitted by TikTok Ireland in respect of changes made after 17 May 2023, including its implementation of Project Clover, when determining which corrective powers are appropriate to exercise in this Decision. As set out below, the DPC has also carefully considered additional information submitted by TikTok Ireland after the

temporal scope of the Inquiry that is relevant to considering the operation of Chinese law during the temporal scope of the Inquiry.

391. I should say that, as noted above, TikTok makes the argument that because temporary or transient processing was inherent to the remote access solution, it should be taken to have addressed the application of the relevant Chinese laws to that processing. There is, I am afraid, no logic to that proposition. The inherent nature of the transient processing only serves to highlight that it is an issue which TikTok were required to address, not that it must have implicitly been addressed.

392. Similarly, the evidence relied on by TikTok in arguing that the DPC erred in its evidence of the Project Clover measures necessarily relate to measures put in place and described after 17 May 2023. In the circumstances, the complaints at Ground 10 do not relate to the infringement finding, only the decision to make the corrective orders.

Arguments

393. In substance, TikTok's claim is that both footnote 113 and the third Xu opinion make clear that the territoriality principle means that the personal data the subject of the Inquiry, *i.e.* the data being transferred to China, is outside the jurisdiction of the Chinese authorities. The third Xu opinion also clarifies that the conclusions in the second Xu opinion about the application of the territoriality principle apply to the data that is processed in China. It contends that the DPC's failure to accept the Chinese law evidence contained in this material was inconsistent with its stated position that it was taking TikTok's Chinese law evidence at its height.

394. In relation to the Project Clover measures, TikTok expressly accepts that the description of those measures at §617 - §644 of the Decision broadly reflect the material provided by TikTok during the Inquiry (see §528 of the grounding affidavit of Elaine Fox) but complain that the assessment of that material was cursory and highlight certain errors. It contends that the DPC appears to have rejected the effectiveness of its measures, in particular in relation to pseudonymisation, without providing reasons for so doing and has made other errors relevant to the assessment of risk.

395. The DPC denies that there was any material error in its assessment of the Project Clover measures which, it contends, was comprehensive.

Discussion – errors in assessment of Chinese law evidence

396. In an appeal on the record, it falls to the court, insofar as it can, to assess the evidence which was before the decision-maker and form its own view on that evidence for the purpose of determining whether the decision-maker has erred. In circumstances where the only part of that evidence with which the DPC engaged in detail was the second Xu opinion, no particular deference should be afforded to the DPC's view, expressed for the first time in these proceedings, that the additional material relied on by TikTok does not adequately address the level of protection afforded to the personal data the subject of the Inquiry in China. In circumstances where it is evidence of Chinese law, it is open to question whether any deference should be afforded to the DPC's views. However, as the issue concerns the application of Chinese law to a particular technical solution, then it seems to me that the DPC's expertise could have some bearing on the question of whether the Chinese law evidence addressed its concerns.

397. Before turning to the material, I note that the DPC correctly concluded that the interpretation of Chinese law was a matter for factual evidence. It did not purport to interpret Chinese law, only whether the evidence TikTok provided showed that its assessment of the level of protection was adequate. I consider that the court's task is the same. The DPC expressly stated that it accepted TikTok's evidence of Chinese law at its height. It did not obtain its own evidence as to Chinese law as part of the Inquiry. In the absence of any contrary evidence, the DPC's decision to accept TikTok's Chinese law evidence at its height was appropriate, there being no basis not to do so.

398. Thus, the only Chinese law evidence which forms part of the record for the purpose of this appeal is that provided by TikTok (I note that there was additional Chinese law evidence before the court for the purpose of the stay application, but neither party has sought to rely on that material in the appeal, and I have not had regard to it). Given the importance of the correctness of TikTok's interpretation of Chinese law to its contention that effectively

equivalent protection was guaranteed, I am forced to question whether the DPC's decision to rely on TikTok's expert evidence was wise. In the context of a lengthy and comprehensive inquiry, I think it would have been prudent for the DPC to have obtained its own advice on this vital issue. The decision not to do so narrowed the scope of the DPC's inquiry to one which, in effect, could *only* consider whether TikTok's assessment was adequate, not whether it was correct. As a result of the DPC's approach, the court is similarly confined to analysing the adequacy of TikTok's assessment on the assumption that what TikTok and its experts say about Chinese law is correct. Insofar, however, as TikTok and its experts draw conclusions from their interpretation of Chinese law as to the level of protection afforded to the personal data the subject of the inquiry, neither the DPC nor this court are bound to accept those conclusions. Furthermore, the DPC was, and the court is, entitled to consider whether the Chinese law evidence is, in fact, addressed to the issues the subject of the Inquiry.

399. The second Xu opinion was provided as part of TikTok's response to the PDD. In the opinion, Professor Xu describes his qualifications:

I hold a PHD in law under the Joint Training of UIBE and University of California, Berkeley. I am one of two initiators of China Personal Information Protection and Data Governance Thirty Person Forum, member of World Data Governance and Cyber Security Research Alliance Secretariat, and a director of China Cyber Information Law Institute. I have published more than 60 papers in Chinese and/or English in reputable law reviews in and outside China in fields such as cyber security, personal information protection, financial technology and data governance. I, as a co-author, have also published On Cyber Sovereignty (Social Science Academic Press, 2017), Big Data, AI and People (Peking University Press, 2019), and other books.

400. He sets out that he was asked to give his opinion on two questions. First, whether Chinese authorities have the power to compel CGEs or their employees to disclose remotely accessible EEA user data that is stored on servers outside China, and second, whether the statement of Chinese law in Section 2 of the December 2022 DTA is accurate. In this regard, it will be recalled that Section 2 of the December 2022 DTA identified divergences between the levels of protection afforded to personal data in China from that guaranteed within the EU but stated that as Chinese authorities were not authorised to compel disclosure of data

that was not stored in China, this did not undermine the effectiveness of the contractual safeguards contained in the SCCs. Questions 1 and 2 were, accordingly, directed to the same issue.

401. Professor Xu states that the opinion responds to the following concerns from the PDD:

(1) “there is a lack of clarity regarding the territoriality principle in Chinese law”, (2) “TikTok Ireland’s submissions, and Data Transfer Assessments, are vague in describing the exact contours of the territoriality principle” *and that, as a result of the deficiencies in (1) and (2), it is unclear* (3) “how the surveillance laws in fact apply in the context of the data transfers”.

402. Having analysed the relevant provisions of Chinese law, Professor Xu concluded that the answer to the first question was that CGEs or their employees could not be compelled to disclose remotely accessible data. In relation to question 2, he opined that section 2 of the December 2022 DTA was an accurate statement of Chinese law as at that date and was consistent with his answer to question 1. Having regard to the content of section 2 of the December 2022 DTA, the response to both questions is to substantially the same effect.

403. Accepting, as I must in light of the evidence, that Chinese authorities cannot require disclosure of personal data stored outside China, does it follow that TikTok has shown that the data transfers the subject of the Inquiry are afforded adequate levels of protection, *i.e.* does it address the local processing concern? In my view, the answer, clearly, is no. As discussed when considering the fair procedures claims at Ground 1, the subject matter of the Inquiry was not data when stored on servers outside China, but data transferred to China by remote access for the purpose of processing. In this regard, the DPC in its submissions correctly distinguished between remotely *accessed* data and remotely *accessible* data. Though TikTok rejected this as a false dichotomy (Transcript Day 10, page 6) it seems to me to be an appropriate, indeed necessary, distinction to make. Completely different considerations arise, or at least could arise, in relation to data which is *capable* of being accessed from China, but which is stored overseas, and data which is *actually* accessed from China and processed there. Put otherwise, the fact that Chinese authorities may not be able to compel access to the former does not necessarily mean that it could not compel access to the latter.

404. TikTok did not suggest that there was nothing in China which was technically capable of being accessed by Chinese authorities. In oral argument, TikTok repeatedly argued that it was the data stored in the overseas servers which was of interest, because, in effect, what was being processed on the computers in China was so transient and piecemeal that it could have no possible interest to Chinese authorities and that any application of the Chinese surveillance laws could only be anticipated in respect of the data stored overseas. That was not established on the record, and is certainly not obvious. It may be, as counsel for TikTok suggest, that the limited form of data relating to an individual user being processed in China would be of little value to the Chinese authorities, but that is beside the point. If Chinese authorities could compel access to *all* the data being processed in China because, to take an obvious example, they were investigating *TikTok*, that would give rise to concerns about whether the protection afforded to personal data was equivalent to that available in the EEA.

405. An adequate assessment by TikTok of the level of protection afforded to data processed or being processed in China was necessary in order for it to comply with its obligations pursuant to Article 46. I can see no error by the DPC in concluding that the second Xu opinion did not address that issue adequately, or indeed, at all.

406. The next material upon which TikTok relies in arguing that the DPC erred in concluding that it hadn't addressed the local processing issue is the July 2024 DTA and, in particular, footnote 113 thereof. Although set out above, for convenience, I will repeat it here:

We have been advised by Fangda and Professor Xu that the transient processing inherent to the facilitation of remote access in China does not alter the above analysis. This is because the relevant data is still stored outside of China (and only remotely accessible from within China) and so is still subject to the requirements set out above. In addition: (i) such transient processing is strictly protected by the constitutional right to confidentiality of correspondence under Article 40 of the PRC Constitution and (ii) such transiently processed data would in any event still be considered offshore data when considering the scope of Chinese authorities jurisdiction (for example as a result of the logic used in Article 4 of Provisions on Data Transfer, released on 22 March 2024).

407. The fact that the information is in a footnote, to which no attention was called by TikTok in its covering letter setting out the material changes in the assessment, tends to undermine the weight which TikTok now seeks to place upon it. A footnote would, I think, typically be understood as providing additional, but not essential, clarification, information or context to the content of the main text. It might also contain a caveat, limiting the apparent scope of the statement footnoted. The content of a footnote should be interpreted in that light. One could not reasonably expect that a footnote would address, by a sidewind, an entirely separate issue than is addressed in the main text. I do not understand footnote 113 to have addressed an entirely different issue here.

408. The footnote can be seen to comprise three separate statements. The first is that the transient processing inherent to the remote access solution does not alter the analysis in the main text. The analysis in the main text was that CGEs and their employees could not be compelled to provide access to data stored overseas. This statement says nothing, therefore, about the local processing issue.

409. The second two statements, (1) that transient processing is protected by Article 40 of the PRC Constitution, and (2) that the data would be considered offshore data because of Article 4 of the Provisions on Data Transfer, could be interpreted as relating to the transiently processed data. However, they are presented as additional reasons why the above analysis – about compellability in relation to data stored outside China – is unchanged, rather than as a separate assessment of the level of protection afforded to the temporarily processed data.

410. Insofar as it can be argued, as TikTok now do, that the footnote addresses the level of protection afforded to the temporarily processed data, I don't think any fair reading of the footnote supports that view. First, and most significantly, the second two statements only tend to reinforce the DPC's concerns that different considerations apply in relation to the transiently processed data and the data stored outside China, *i.e.* they tend to confirm the entire basis of the DPC's remaining local processing concern: the fact that data *stored outside* China is protected does not automatically translate into data *processed inside* China being subject to the same protection. Insofar as the statements then purport to address the *different* position of transiently processed data, there is no assessment equivalent to, or even approaching the type of assessment carried out by TikTok in relation to the data stored outside China. Neither statement is to the effect that the Chinese authorities are not entitled

to access data being processed in China, rather they assert either that it has some level of protection under Article 40 of the PRC Constitution, and that it is regarded as offshore data for the purpose of Article 4 of the Provisions on Data Transfer.

411. Neither statement could be said to provide any significant comfort and fall far short of showing, or even, asserting that essentially equivalent protection is guaranteed. It has never been suggested that personal data is afforded *no* protection in China, so the fact that transiently processed data is protected under the PRC Constitution establishes nothing. As the DPC points out in its written submissions, the July 2024 DTA itself notes that Article 40 is subject to an exception in “*cases necessary for national security or criminal investigation.*” The second statement, referring to the classification of transiently processed data as “*offshore data*” isn’t explained at all and appears speculative, relying as it does on the “*logic*” of Article 4. At most, this statement provides a hint of a basis for contending that the locally processed data falls outside the scope of the relevant Chinese laws. Although it was stated on TikTok’s behalf during oral submissions that “*offshore*” only has one meaning (Transcript Day 2, p. 47), it will be apparent when we review the third Xu opinion that, in fact, as Professor Xu explains, in his view, it has a very particular meaning as a matter of Chinese law.

412. Tellingly, neither in the footnote, or anywhere else until the third Xu opinion does TikTok assert, still less explain, that data transiently processed in China is subject to essentially equivalent protection to that guaranteed within the EU. No one could reasonably be expected to accept that to be the case by reference to footnote 113 of the July 2024 DTA and in those circumstances, I cannot conclude that the DPC erred in concluding that the corrective orders were required in light of the July 2024 DTA (or any of the DTAs).

413. By contrast to the second Xu Opinion and footnote 113, the third Xu Opinion addresses in terms the level of protection afforded to the transiently processed data, in particular whether Chinese authorities could compel access to that data. Before turning to that opinion, it is helpful to return to the DPC’s fourth RFI and the information provided by TikTok in response thereto which is expressly referenced in the third Xu opinion.

414. It will be recalled that in its fourth RFI, the DPC requested details of the technical mechanism by which TikTok gave effect to the remote access solution. In its response dated

11 March 2024, TikTok provided additional detail of what was involved. This information was not discussed in detail at the hearing of the action, indeed TikTok suggested that no reliance was being placed on it. Much of it is subject to the confidentiality order made on 20 February 2026. I will refer to what appear to be significant features in outline terms here.

415. Of particular note is that there is a section headed ‘*Storage and Processing*’. In that section, TikTok explain that making the remote access connection results in data being “loaded” into the RAM (random access memory) of the devices of the CGE employees. The data will also be processed on the CPU (central processing unit) and GPU (graphical processing unit) of those devices, including any transitory processing within the cache memory of those processing units. This is described as an “*inevitable consequence of any remote access solution*”.

416. The response describes that RAM is for a transitory period, while needed for the programme or process involved and is cleared when the programme or process ends. It is overwritten when RAM is required for new processes. It is only retained when the devices are powered and is “*normally*” lost when the devices are shut down. It is explained that RAM is fragmentary and that even if directly accessible, it would be “*unfeasibly complex*” to reconstruct the data in any coherent form.

417. It is stated that [REDACTED]

[REDACTED]. It refers back to a similar statement to this effect in the response to the PDD in which this [REDACTED] is described as one of the new measures introduced by Project Clover “*which did not form part of the pre-existing measures*”.

418. I note that in the Decision (at §129), the DPC summarises this information as it being TikTok’s position that the remote access solution does not result “*in the storage, in any form, of that personal data in China.*” The contents of the 11 March 2024 response to the fourth RFI are not, in my view, nearly so unequivocal.

419. The next heading is ‘*Temporary Storage and Caching*’. The response suggests that TikTok has considered whether “*the temporary browser storage configurations that are inherent in internet usage might result in the storage of EEA user data.*” It identifies ‘temporary storage’ and ‘temporary cache’ as browser storage locations. The response

contains a bald statement that TikTok has considered the temporary storage configurations for the main applications used by the remote access solution and that these do not contain EEA user data. It says that it is not aware of EEA user data being temporarily cached but it is conceivable that some files might be. [REDACTED]

420. The response expressly accepts that the processing of data in China is processing within the meaning of Article 4 of the GDPR.

421. As noted in his third opinion, Professor Xu was asked to consider:

Whether, in the specific circumstances of the transfers the subject of the Inquiry, Chinese authorities have the power to compel China Group Entities (or their personnel in China) to disclose EEA User Data temporarily processed in the computer information systems in China of the relevant China Group Entity personnel as a result of remote access to EEA User Data stored on servers in Singapore, Malaysia and the United States (“Question 1”).

422. He was also again asked to consider whether the statement of law in the most recent DTA, the July 2024 DTA, was an accurate statement of Chinese law.

423. The question of whether disclosure of data being processed in China can be compelled by the Chinese authorities is, therefore, directly addressed in the third Xu opinion. But his the analysis, rather than showing that the DPC’s concerns that this issue had not been addressed were misplaced, tends to confirm that the DPC was correct to consider that the issue had not previously been addressed, and entirely justifies the DPC distinguishing between remotely accessible and remotely accessed data. The reason for Professor Xu’s conclusion that disclosure of remotely accessed data cannot be compelled requires an entirely different analysis than did his conclusion that Chinese authorities couldn’t compel access to data stored outside China and is not based on a straightforward application of the territoriality principle. In particular, it requires Professor Xu to explain that as a matter of general principle “Chinese law treats the data from a foreign State that is temporarily processed within China as a result of a remote access solution as overseas data (i.e. as or

in the same way as other data that is not stored in China”). Perhaps ironically, this proposition is explained in a footnote:

In Chinese legal practice, data that originates outside China without introducing any personal data originated in China is referred to as “offshore data”, a special type of oversea data. Chinese authorities consider that PRC laws, particularly those related to the security management of outbound data transfers, are not applicable to offshore data. (See Yanqing Hong, The “Rebalancing” of China’s Data Export Security Management System - A Perspective on Data Competition Strategies Between Countries, 3 Chinese Legal Review.) As an example supporting this legal practice, the Hainan Free Trade Port International Data Center Development Regulations (effective on 1 December 2024) explicitly exempt from the PRC data export management regime the processing of “offshore data” during offshore data centre business conducted in China. The corresponding official statement from the PRC regulators stated that these rules were formulated to support offshore data centre business and promotes cross-border data flows. (See <https://www.hainan.gov.cn/hainan/dfxfhg/202411/f6f58aed43374fe8afcd36ae68dc117.shtml?ddtab=true> and https://db.hainan.gov.cn/jdhy/zxjd/202412/t20241203_3778885.html).

424. The remaining portion of the third Xu opinion which sets out Professor Xu’s basis for concluding that the temporarily processed data will be treated in the same way as data stored overseas is relatively brief and so can be set out here in full:

The scope of the jurisdiction of Chinese law in relation to overseas data, in light of the territoriality principle, can be further understood by reference to an example. Article 4 of the Provisions on Promoting and Regulating the Cross-border Data Flow clarifies that a data handler is not required to fulfill obligations under Chinese law applicable to the cross-border transfer of data if the data is collected and generated outside China, transmitted to China for processing, and then returned back outside China, provided no personal information or critical data from China is introduced into the processing. Because EEA User Data is collected and generated outside China and will only be temporarily accessible and processed in China as part of the remote access solution (for temporary processing by engineers independent of their other processing activities

within China), it is categorized as overseas data according to these provisions. In other words, the EEA User Data temporarily processed in the computer information systems in China of the relevant China Group Entity personnel as a result of remote access to EEA User Data is treated the same way as any other data stored outside China.

425. Having concluded that the data will be treated the same way as any other data stored outside China, Professor Xu then, effectively, repeats his analysis of the relevant Chinese laws contained in his second opinion, save that he adds in respect of each law, that just as Chinese authorities have no jurisdiction over data stored overseas, they have no jurisdiction over data temporarily processed in China because data “*temporarily processed on computer information systems in China as a result of the remote access qualifies as overseas data*”.

426. He provides a summary of his opinions. In addition to concluding that the July 2024 DTA contains an accurate statement of Chinese law, he concludes in relation to the first question he was asked that:

In response to Question 1, my opinion is that Chinese authorities do not have the power to compel China Group Entities, or personnel in China working for them, to disclose EEA User Data temporarily processed in the computer information systems in China of the relevant China Group Entity personnel as a result of remote access to EEA User Data stored on servers in Singapore, Malaysia and the United States, in the specific circumstances of the transfers the subject of the Inquiry, as described above at Section C and in the letter from TikTok to the DPC dated 11 March 2024.

427. This response confirms that Professor Xu is addressing the technical solution being relied on by TikTok as described in its response to the fourth RFI.

428. It is worth highlighting some features of the opinion. First, on its face, it does appear to address the very issue which the DPC said had not been addressed at any time by TikTok up to the date of infringement and beyond and provides a clear statement that the data being processed in China is not subject to the relevant Chinese laws and, therefore, essentially equivalent protection is available.

429. Second, and critically, Professor Xu’s analysis is wholly at odds with TikTok’s contention that the locally processed data had been addressed all along. The entire basis of

TikTok's contention that the remote access solution (with other measures) guaranteed equivalent protection is that the territoriality principle meant that the EEA user data fell outside the jurisdiction of the Chinese authorities because it was stored overseas. The third Xu opinion suggests that the EEA user data processed in China is outside of the jurisdiction of the Chinese authorities because Chinese law is, in effect, *disapplied* in relation to that data.

430. Although the local processing issue *is* addressed in the opinion, the basis for Professor Xu's conclusions is far from compelling. He identifies that data processed in China is treated as overseas data in a very limited context, notably a measure introduced after the July 2024 DTA which was not, therefore, capable of supporting a conclusion that for all purposes, or more pertinently, for the purpose of the transfers the subject of the proceedings, *i.e.* the transfers during the temporal scope, the data processed in China would be treated in the same way as data stored outside China. Moreover, the measure relates to the *export* of data. The main text refers to the treatment of overseas data, again by way of an example only, Article 4 of the Provisions on Promoting and Regulating the Cross-border Data Flow, a measure contingent on no "*critical data*" being introduced in China. It is far from clear from these examples how TikTok, or Professor Xu, extrapolates that the comprehensive form of protection which it contends applies to TikTok's EEA user data stored overseas, also applies to its EEA user data being processed in China.

431. I note that in the section of his opinion headed "*Summary of my previous opinions*", Professor Xu asserts that the "*principles set out in my Second Opinion extend to such temporary processing in China as a result of remote access.*" However, nowhere in his opinion does he provide any basis for contending that the underlying principle informing his second opinion – that the data is stored overseas and therefore outside the jurisdiction of the Chinese authorities – applies to the data being processed in China. Rather, he introduces a new argument, that for the reasons he explains, Chinese authorities will treat the temporarily processed data *as if* it were stored overseas.

432. It will be recalled that the main basis for TikTok's contention that the EEA user data transferred to China is afforded equivalent protection to that guaranteed within the EU is that the data is not stored in China and, therefore, as a matter of Chinese law, it cannot be accessed by Chinese authorities. That being so, in order for TikTok to rely on the *same*

principle to suggest that data actually processed in China is also guaranteed equivalent protection, it would have been necessary for TikTok to assert that the data being *processed* in China was not *stored* there *as a matter of Chinese law*. As noted above, English-language dictionary definitions of what storage meant would have no relevance to such an analysis. Such an analysis would no doubt require engagement with details of the particular technical solution employed by TikTok and the details of the response to the fourth RFI. As an aside, one might plausibly query whether any lawyer, irrespective of their technical knowledge, could be regarded as qualified to provide such an opinion without the benefit of expert technical opinion, though I do accept that Professor Xu appears to have significant experience of such matters.

433. There is no need to consider whether Professor Xu was qualified to offer such an opinion, because, critically, he doesn't do so. As we have seen, having been briefed as to the precise technical means by which the data transfers occur, he does not argue that the data processed in China is outside the jurisdiction of Chinese authorities because the data isn't stored there, rather he argues that it is subject to special treatment pursuant to particular laws and is treated *as if* it is stored overseas. TikTok's argument, that all personal data is *actually* stored overseas and therefore outside the jurisdiction of the Chinese authorities, does not, therefore, provide an answer at all for the data processed in China. I note that this only serves to highlight the fallacy of TikTok's assertion that because it had addressed the position of data stored overseas, it should be taken to have implicitly addressed the position of the data processed in China. The third Xu opinion illustrates that it had not.

434. I note that one of the other criticisms the DPC makes of the third Xu opinion, that it focuses on the risk of compelled disclosure and does not "*address other means by which Chinese public authorities may secure access to EEA Data*" does not appear well made. The opinion addresses the actual concerns articulated by the DPC in the PDD and in the Decision. The DPC had not, before the Decision, specified any concern regarding "*other means*" of access. In this regard, there was a suggestion at the hearing that controllers should have known, in light of the decision in *Schrems II*, of the possibility of the type of State surveillance at issue in that case and addressed that risk in their DTAs. That may be so, but if there was any concern by the DPC that TikTok's DTAs did not address such risks, it failed to articulate it, or at least failed to articulate it sufficiently that any failure could have

justified a finding of infringement without affording TikTok a further opportunity to comment.

435. Accordingly, on the evidence on the record by March 2025, TikTok had addressed the issue which led to the finding of infringement, the absence of an assessment of the level of protection afforded to EEA user data processed in China. The conclusion of the third Xu opinion on this issue is unequivocal. The explanation for why that is so is, however, not convincing. This is not to offer an interpretation of Chinese law, which is far beyond the remit of this court, but rather an observation on whether the legal opinion advanced by Professor Xu is adequately supported by logic and evidence.

436. TikTok seem to suggest (Transcript, Day 10, pp. 109/110) that, because the DPC had indicated that it was taking TikTok's Chinese law evidence at its height, the third Xu opinion must also be taken at its height. That does not follow. The Chinese law evidence is evidence of fact. The DPC was entitled to consider that evidence and determine if it found it persuasive, even in the absence of contrary evidence. The fact that it opted, perhaps unwisely as I have suggested above, to accept the Chinese law evidence set out in the DTAs and in the first and second Xu opinions without obtaining its own Chinese law advice, did not bind the DPC to accept any subsequent evidence. More importantly, it does not require the court, in an appeal on the record, when assessing the evidence, to uncritically accept it. There is no principle that a court is required to accept opinion evidence as to foreign law which is unconvincing or based on weak logic.

437. Before considering what the consequences of the foregoing are, I will consider the assessment of the Project Clover measures the subject of the pleas at Ground 10

Discussion – errors in assessment of Project Clover

438. At Ground 10 of the grounds of appeal, TikTok allege, in effect, two errors by the DPC in its assessment of the Project Clover measures.

439. First, it contends that the DPC erred in its identification of what “*private and sensitive*” data is remotely accessible. Second, it contends that the DPC's rejection of the pseudonymisation measures adopted by TikTok as ineffective was based on an erroneous

assumption that no data could remain in plaintext if pseudonymisation was to be effective and that its conclusion in relation to pseudonymisation was otherwise unexplained.

440. In circumstances where TikTok accept that the DPC’s description of the Project Clover measures at §617 - §644 of the Decision “*broadly reflects*” the material submitted (subject to the errors identified), it is convenient to consider those measures by reference to how they are described in the Decision.

441. At §618, the Decision describes the key goals of the Project Clover, as set out in the Project Clover Report. These were:

- i. Data localisation: Store EEA User Data by default in data centres in Ireland and Norway.*
- ii. Access controls: Build security gateways and controls to monitor and prevent unauthorised user access.*
- iii. Minimise data flows: Build security gateways and controls to monitor and prevent unauthorised data transmission.*
- iv. Co-management solution with independent third party security provider: Work with a third party security provider to operate security gateways and controls, perform security monitoring, and validate data transmission and user access.*
- v. Auditability of the solutions: Provide a solution that is auditable and allows third party oversight and review.*

442. And at §619, the Decision sets out what TikTok claimed was the effect of Project Clover in its response to the PDD:

- 1. Protected Data in the European Enclave will not be accessible by China Group Entities or their employees (TikTok has already implemented this step for New Protected Data as part of its Current Measures, utilising the Temporary European Enclave and the European DSM);*
- 2. China Group Entities will only have access to Excepted Data in the Global Data Centres;*
- 3. Excepted Data in the Global Data Centres will be subject to access controls, as well as privacy enhancing technologies, including differential privacy and*

pseudonymisation measures. TikTok will complete this step through the implementation of its In-Progress Measures as described (and in accordance with the timescales set out) in the Project Clover Technical Report.

- 4. TikTok will apply privacy enhancing technologies, including anonymisation measures (differential privacy) and pseudonymisation measures (through encryption-on-access and redaction of key identifiers), to Excepted Data upon access by employees of China Group Entities.*
- 5. Legacy Protected Data will be deleted from the Global Data Centres, with the result that China Group Entities will not have access to any Protected Data.*

443. The Decision expressly accepts that TikTok has made “*significant changes*” to the manner in which it transferred data. It then summarises those changes.

444. First, all personal data is now stored on servers in what it calls the European Enclave, *i.e.* outside China (there was some debate at the hearing about whether this process had been completed, though nothing turns on this for present purposes).

445. Second, a distinction was made between “protected data”, which is not remotely accessible, and “allowable data” which is. As set out above, allowable data is made up of “public data”, “interoperable data”, and “aggregated data”. Measures are in place, which are audited, to ensure that no protected data is accessed by the CGEs.

446. Third, the Decision then sets out the purposes for which data is accessed and fourth, the categories of data which are accessed. The categories are set out in tables of public data, interoperable data and aggregated data. In respect of each category, the table identified what, if any, level of encryption is applied. The levels are identified as ‘encryption’, ‘redaction’, ‘encrypt city, outside of “information isolated island”’, and ‘none’.

447. Fifth, the Decision addresses the format of personal data accessed by CGE employees (at §634):

The July 2024 Data Transfer Assessment records that the format of the personal data the subject of the transfer and which may be remotely accessed by the China Group Entities may be “Encrypted /Pseudonymised / Plain-text”... The Global Operations Gateway controls how that data is made available to employees of the China Group

Entities. When employees in China consult EEA User Data, TikTok Ireland stated that it applies encryption or redaction to the main identifiers associated with a user. The list of identifiers that are encrypted or redacted is set out above in the section setting out the “Categories of personal data the subject of remote access following changes implemented by TikTok Ireland after the Preliminary Draft Decision”. TikTok Ireland submitted that, regarding data remotely accessed, this means that employees in China see an encrypted value or data that is entirely blocked for these identifiers, which enables those employees to carry out work without having sight of those identifiers.

448. Finally, the Decision outlines the additional controls on access implemented since the date of the PDD.

449. The first error identified by TikTok relates to the categories of information which the DPC concluded were accessible by remote access. At §689 of the Decision, the DPC sets out the types of material which can be accessed:

The categories of EEA User Data subject to the Data Transfers on an ongoing basis also includes personal data that may be private and sensitive to a user. As set out above, these categories include personal data such as: the age level of users; who those users follow and are followed by; details concerning whether a user has been subject to moderation; a record of the user’s behaviour on the TikTok platform, including timestamps relating to same; user generated content, including their videos, images, comments, and metrics relating to same, as well as moderation status of that content; reports, bans, and penalties imposed further to User Support and User request; general location; and their direct message content. TikTok Ireland’s European Transfer Matrix, dated 6 December 2024, states in respect of the transferred data, that “It is generally not the intention of TikTok to collect any Sensitive Data, however Sensitive Data may be collected incidentally or uploaded by the User”. The DPC finds that these categories of EEA User Data on an ongoing basis include personal data that may be private and sensitive to a data subject.

* emphasis added

450. TikTok accepts that most of the categories of data identified by the DPC are accessible by remote access but argues that “*not all of them appear to be of a high sensitivity*” (affidavit of Elaine Fox at §529). However, it says that the DPC has erred in concluding that the two highlighted categories of data, general location and direct message content, which it accepts may be “*private and sensitive*” are accessible. It contends that only “*approximate*” location data was collected during the temporal scope of the Inquiry. It says that direct message content was not available by remote access at all during the temporal scope.

451. The DPC accepts that precise location data is not remotely accessible, but disputes TikTok’s contention that general location data is not capable of being sensitive in certain circumstances. It accepts that it erred in referring to direct message content and pleads that it should have referred to ‘direct message data’, though the distinction is not explained on affidavit. The DPC argues, however, that it has identified significant categories of data which were remotely accessible and which could be considered private and sensitive depending on the circumstances.

452. Although the errors identified by TikTok and accepted by the DPC are unfortunate, minor errors are perhaps inevitable in a process as complex and extended as was the Inquiry. In an appeal, the onus of proof is on TikTok to establish that the errors identified were, or were capable of, being material to the Decision. It has not discharged that onus. The errors in identifying certain private and sensitive data as accessible by the remote access solution certainly *appear* minor and must be considered in the context of the DPC identifying a number of other categories of data which could be private and sensitive and which TikTok does not dispute were accessible. The data which is accessible may be, as TikTok suggests *less* sensitive than the categories of data which are not accessible, but it was certainly within the expertise of the DPC to determine that the data which is transferred could be private and sensitive, and any minor errors by the DPC in identifying all the categories of data so transferred does not undermine its overall conclusion at §690 of the Decision.

453. The more substantial issue raised by TikTok relates to the DPC’s treatment of the pseudonymisation measures now forming part of Project Clover. In this regard, it should be noted that even prior to Project Clover, certain of the data transferred to China was pseudonymised as detailed in TikTok’s early DTAs. Project Clover appears, therefore, to

have involved a development of those measures, and certainly, following the adoption of the Project Clover measures, pseudonymisation is applied in a changed context.

454. The mechanisms are not described in detail in the Decision. A comprehensive explanation of the pseudonymisation and differential privacy measures put in place by TikTok are contained in the Project Clover Report submitted in response to the PDD. Professor Mittal provided a report at the same time confirming the effectiveness of TikTok's differential privacy policy.

455. The DPC did not raise any queries regarding this material following its receipt, including in their fourth RFI dated 8 February 2024, and did not, despite request from TikTok, meet with it for the purpose of discussing same.

456. As it had flagged in its letter of 14 February 2025, prior to the Draft Decision, TikTok provided an update on Project Clover prior to the Decision, though it provided it on 11 April 2025 rather than 10 March 2025 as indicated. The Decision states that the DPC had regard to this update. Unlike the third Xu opinion, the DPC has not sought to “contextualise” that statement.

457. The update is an almost 50-page document which explains in detail not only the steps taken by TikTok in relation to the pseudonymisation of data transferred to China, but also the role of NCC Group in monitoring the steps employed and identifying weaknesses. The report does not directly address the question of whether personal data is subject to essentially equivalent protection to that guaranteed in the EEA by virtue of the Project Clover or pseudonymisation measures. That does not appear to have been asserted by TikTok in any of the material submitted by it. It does however refer to the testing done by NCC:

NCC Group also assessed the likelihood of reidentification in the event an attacker is able to obtain a dataset containing all the Allowable Data accessible by CGE Personnel about a user. In particular, they considered the following scenarios, including how the leaked dataset could be linked with external data:

- 1. Given a dataset, can a member of that dataset be directly re-identified?*
- 2. Given a dataset, can it be inferred that a user is contained within that dataset?*

3. *Given a specific user in a dataset, can any additional non-public information be learned about that user?*

458. Notably, the testing assumes an “attacker” obtaining all the allowable data about a user, thus all data whether encrypted or in plain text. The document, oddly, does not immediately indicate the outcome of those assessments. However, later in the document, the following is stated:

NCC Group's testing has to date found that the solution does not enable reidentification of an EEA User.

459. This conclusion appears consistent with that in the Mittal report. The Mittal report is referred to but not addressed in the Decision in the assessment of the Project Clover measures.

460. As set out above at Ground 1, TikTok’s complaint is about how all this information was dealt with by the DPC at §690 of the Decision where it appears to have concluded as a matter of *fact* that TikTok had not established the effectiveness of the pseudonymisation measure because pseudonymisation does not necessarily prevent re-identification.

461. As counsel for TikTok put it, this analysis simply begs the question. Of course, says TikTok, pseudonymised data *may* still constitute personal data if the data combined with additional data can identify a data subject. This follows from the definition of pseudonymisation in Article 4(5). The question the DPC should have addressed is whether, in fact, data subjects can be identified. The DPC’s conclusion that TikTok has not demonstrated that they cannot be identified is not explained.

462. The DPC identifies case law which refers to the high threshold for establishing that pseudonymisation is effective. Case C-413/23P, *European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB)*, a case concerning an equivalent Regulation to the GDPR which applies to Union institutions. The case concerned the processing of personal data by the SRB and, in particular, the question of whether pseudonymised data sent by the SRB to a third party, Deloitte, for the purpose of carrying out an analysis should be regarded as personal data.

463. The SRB had placed a Spanish bank, Banco Popular Español SA, in resolution. A question arose as to whether the creditors and shareholders of the bank were entitled to compensation, and this depended on the question of whether they would have done better in an ordinary insolvency. SRB engaged Deloitte to carry out the necessary analysis.

464. A process of engagement with the shareholders and creditors to determine if they were entitled to and wished to be heard took place. This was in two phases, a registration phase in which the shareholders and creditors provided personal data for the purpose of establishing their right to be heard, and a consultation phase in which those who had an entitlement to participate had an opportunity to submit comments.

465. Only the comments, identified by alphanumeric codes, were transferred to Deloitte. Only the SRB retained the information which would have enabled a particular comment to be attributable to a particular person. The EDPS, nonetheless, concluded that Deloitte had been the recipient of personal data and found a breach of Article 15(1) of the GDPR. The SRB appealed to the General Court which annulled the decision of the EDPS concluding that the information transferred to Deloitte was not personal data. The EDPS appealed in turn to the CJEU. In particular, it challenged the General Court's conclusion that the comments transmitted did not relate to "*identifiable*" persons. In substance, the EDPS argued that pseudonymised data should always be treated as relating to an identifiable person.

466. The CJEU observed (at §69) that:

"... it must be borne in mind that, under Article 3(1) of Regulation 2018/1725, information must relate to an 'identified or identifiable' natural person in order to be classified as personal data within the meaning of that provision. Accordingly, the application of that regulation presupposes, in principle, an examination of whether the data subject is identified or identifiable by the information in question."

467. The CJEU noted that the definition of pseudonymisation presupposed the existence of information which would enable the identification of data subjects. However, it stated (at §74 and §75):

“The fact remains that, in the third place, the requirement that the identifying information be kept separately and that it be subject to technical and organisational measures ‘to ensure that the personal data are not attributed to an identified or identifiable natural person’, laid down in Article 3(6) of that regulation, indicates that the objective of pseudonymisation is, among other things, to prevent the data subject from being identified solely by means of pseudonymised data.

Accordingly, provided that such technical and organisational measures are actually put in place and are such as to prevent the data in question from being attributed to the data subject, in such a way that the data subject is not or is no longer identifiable, pseudonymisation may have an impact on whether or not those data are personal within the meaning of Article 3(1) of Regulation 2018/1725.”

468. The Court referred to the recital in the 2018 Regulation equivalent to Recital 26 quoted above and observed (at §79):

“.... in order to determine whether a natural person is identifiable, account should be taken of ‘all the means reasonably likely’ to be used by the controller or by ‘another person’ to identify the natural person ‘directly or indirectly’. In addition, the fourth sentence of that recital sets out that, to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of ‘all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”

469. The Court concluded on this issue (at §85 and §86) that:

“Consequently, in the light of the case-law referred to in the preceding paragraph, the EDPS is incorrect in so far as he submits that the fact that pseudonymised data are not, as the case may be, personal in nature for persons to whom the controller transfers the pseudonymised data makes it unduly possible to remove those data from the scope of EU law on the protection of personal data. According to that case-law, that fact has no bearing on the assessment of the personal nature of those data in the context, inter alia, of a potential subsequent transfer of those data to third parties. Accordingly, in so far as it cannot be ruled out that those third parties have means reasonably allowing them

to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.

It follows that, contrary to what the EDPS maintains, pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725, in so far as pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.”

470.Notwithstanding that conclusion, the CJEU ultimately concluded that the data transmitted to Deloitte was personal data because *“the identifiable nature of the data subject must be assessed by putting oneself in the controller’s position. It is not disputed between the parties that the SRB had, as controller, all the information necessary to identify the authors of those comments. It follows from the foregoing that, contrary to the SRB’s contention, the information at issue constitutes personal data.”*

471.The DPC is correct insofar as the SRB Decision highlights the high threshold for establishing that pseudonymisation is effective. However, it is also authority for the proposition that pseudonymised data is not necessarily personal data.

472.The DPC’s consideration of pseudonymisation, and the Project Clover measures generally, arose in its consideration of whether a suspension order was warranted. The DPC acknowledged in the Decision that any corrective order had to be appropriate, necessary and proportionate. Having regard to the two-year gap between the temporal scope of the Inquiry (as fixed by the DPC) and the actual making of the corrective order, and the significant changes which the DPC accepted that TikTok had made in relation to the data transfers in that period, it was, in my view, not open to the DPC to summarily reject the effectiveness of the pseudonymisation measures employed by TikTok in deciding that a suspension order was necessary. This, unfortunately, is what it appears to have done.

473.It is worthwhile contrasting the explanation for the DPC's conclusion that TikTok had not demonstrated the effectiveness of the remote access solution in the context of the data transfers with its explanation of its conclusion in relation to the differential privacy and pseudonymisation measures. The former is explained repeatedly in the Decision, the latter, not at all

474.I entirely accept that the DPC, in the exercise of its technical expertise, was entitled to form the view that the pseudonymisation was ineffective, or that its effectiveness had not been established by TikTok. Indeed, it may have been open to the DPC to conclude that *even if effective* the suspension order was necessary in light of its conclusion regarding the failure to assess the local processing issue, or, perhaps, because the pseudonymisation and differential privacy solutions were not comprehensive. But it had to have reasons for so doing, and, furthermore, to provide those reasons in the Decision. Its failure to do so was a clear error on its part. It does not explain why it rejected the apparent conclusions of the Mittal Report or the NCC report or, if it accepted them, why those conclusions were immaterial to its consideration of whether to make the suspension order.

Overall conclusions on Ground 2 and 10

475.I have, accordingly, concluded that there were errors by the DPC in the manner in which it assessed the question of whether TikTok had addressed the local processing issue in light of all the evidence which was available to it at the time that it made the Decision. There was also an error by the DPC in the manner it addressed TikTok's evidence regarding the application of pseudonymisation measures.

476.As noted, the errors are clearly not relevant to the infringement finding in relation to Article 46, or the decision to impose an administrative fine for that infringement, and can have no bearing on that aspect of the DPC's decision. Whether those errors are sufficient to warrant the court substituting a different form corrective order to that imposed by the DPC will be addressed in the final section of this judgment.

Ground 11 – Error in making the corrective orders

477. As referred to above, in addition to the errors of law and fact relied on by TikTok, it contends that the decision to make the corrective orders was not justified in this instance. It also argues that the processing order was unclear and that the time for compliance was inadequate.

Arguments – ground 11

478. TikTok advanced four arguments under this heading. As referred to above, it contends that the DPC misinterpreted *Schrems II* as imposing an obligation to suspend transfers where there has been a finding of non-compliance, which it says is incorrect in the context of a finding that there has been an inadequate assessment as opposed to a finding that there was ineffective protection in the third country. That issue has been addressed above under Ground 3 where I concluded that notwithstanding the references in the Decision to a duty to suspend by reference to *Schrems II*, the DPC in fact carried out an assessment of whether a suspension order was proportionate in this instance.

479. Second, TikTok argues – in apparent acknowledgement of the fact that the DPC *did* consider whether the suspension order was proportionate – that the DPC erred in its conclusion that it was. It argues that the DPC should have ordered it to submit a new DTA rather than make the suspension order.

480. Third, it argues that the DPC could not make a suspension order in the absence of a finding that there was an ongoing infringement.

481. It argues that the processing order is uncertain in breach of the requirement for legal certainty. In this regard, it refers to the decision in Case C-570/19, *Irish Ferries* (at §164):

It should be noted at the outset that the principle of legal certainty is a fundamental principle of EU law which requires, in particular, that rules should be clear and precise, so that individuals may ascertain unequivocally what their rights and obligations are and may take steps accordingly...

482.In the domestic context, it refers to the decision in *Tallon v DPP* [2023] IECA 125, a case concerning the validity of a civil order made pursuant to s. 115 of the Criminal Justice Act 2006, a provision which permits a District Judge to make orders to prohibit a person from doing anything specified in the order. The order in question prohibited the applicant from engaging in public speaking and recording in the environs of Wexford Town. The order was quashed as uncertain. The court noted (at §115) that:

“Applying the principle that an order that imposes an obligation to abide by it on pain of criminal sanction, must be clearly expressed and indicate precisely what the subject of the order is required to do or refrain from doing, I am satisfied that this civil order was correctly held by the High Court to violate the principle of legal certainty.”

483.TikTok accepts that it does not face a criminal prosecution for failing to comply with the processing order, but says that it could face an administrative fine which should be regarded as punitive in nature.

484.Reference was also made to the decision in *Dundalk Town Council v Lawlor* [2005] 2 ILRM 106, a case stated in which the High Court held that a planning enforcement notice which required the respondent to “*return site to its previous condition*” within a period “*immediately commencing*” on the date of the notice was invalid. As with the order in *Tallon*, failure to comply with an enforcement notice could lead to criminal prosecution. The court concluded that the time period was impossible to comply with and the terms of the notice were insufficiently clear.

485.Finally, TikTok contends that six months does not afford it sufficient time for compliance with the corrective orders.

486.The DPC denies all of these complaints. As already determined, it says it considered the proportionality of the suspension order and in the absence of an assessment which showed that the personal data being processed in China was subject to essentially equivalent protection, that the suspension order was the least onerous means of achieving the objectives of the GDPR. Insofar as TikTok argues that the DPC should have requested a fresh DTA, the DPC is at pains to highlight that despite the offer of an updated DTA in May 2025 correspondence, TikTok still has not provided such an update.

487. It says that there is no uncertainty about what the processing order requires. Finally, it says that six months to comply with the corrective orders was appropriate and proportionate.

Discussion – ground 11

488. As concluded above, it is clear that the DPC did assess whether to make a suspension order and treated itself as having a discretion. Having regard to the gap between the temporal scope and the suspension order, and the acknowledged changed in circumstances in that period, that was, in my view, entirely appropriate.

489. I cannot see any substance to the argument that the DPC should have requested a further DTA rather than make the suspension order. To reiterate, the default position is that the transfer of personal data to third countries is impermissible unless equivalent protection can be guaranteed. It is possible, *per* the Supplementary Measures Recommendations, to transfer data where such protection is not guaranteed, where it can be demonstrated that there is no reason to believe that relevant laws will be applied in practice. However, it is an essential prerequisite to that determination that the scope of the relevant laws is properly assessed.

490. The DPC had concluded that TikTok had not assessed the level of protection afforded to data processed in China under the relevant Chinese laws. Even accepting TikTok's evidence that no requests for personal data had been made by Chinese authorities and that the data would be of no use or interest to the Chinese authorities, unless and until there was an adequate assessment of the application of those laws to the data processed in China, no proper determination could be made of whether there was a risk of those laws being applied in practice. TikTok had been given many opportunities to address the issue and had updated its DTA four times without so doing (as I have concluded above). The *remedy* for this failure was not to permit TikTok to continue to transfer data and provide it with a further opportunity to address the issue which it had failed to address. Requiring it to submit a fresh DTA would not have met the objectives of the GDPR.

491. The argument that the DPC could not make a suspension order without making a further finding of infringement is not well made for a variety of reasons. First, having determined

that there was an infringement, the DPC was *obliged* by section 111 of the 2018 Act to decide whether a corrective order should be made. These are necessarily sequential. To take TikTok's argument at its height would lead to some form of Zeno's paradox, where the DPC was never in fact permitted to reach a determination on corrective orders.

492. The position in this case was unusual, in large part because of the DPC's decision to limit the temporal scope of the Inquiry. However, the DPC addressed this complication by considering whether the issues which led to the finding of infringement had been addressed by the time the decision on whether to make a corrective order was made. It concluded that they had not been. I can see no error by the DPC in this approach.

493. There is no ambiguity or vagueness about the processing order. The processing order requires that TikTok bring its processing into compliance in the manner detailed in the Decision. The Decision clearly explains that the processing which is *non-compliant* is the transfer of personal data to China in the absence of an adequate assessment which confirms that the data will be subject to essentially equivalent protection in China. There can have been no doubt in TikTok's mind how to comply with that order, or looked at from the opposite perspective, what conduct would lead it to breach that order. The order does not suffer from the same ambiguities as those in *Tallon* or *Lawlor*.

494. I note that following the Decision, TikTok sought to engage with the DPC regarding what was required by the corrective orders, and TikTok criticises its failure to do so. The DPC in turn criticises TikTok for not having submitted a revised DTA, suggesting it seems that TikTok's complaints ring somewhat hollow.

495. Although I have concluded that the processing order is not invalid for vagueness, I do think that it would have been helpful had the DPC engaged with TikTok as requested in correspondence to enable it to understand whether there were measures it could take which would prevent the suspension order 'biting'. I cannot see any legislative barrier to it so doing, and such engagement appears consistent with the obligations imposed on supervisory authorities imposed by Article 57 of the GDPR to promote awareness of controllers and processors of their obligations under the GDPR. It might also have been helpful for TikTok to submit the revised DTA which it had offered, notwithstanding the lack of engagement.

Had both parties engaged constructively, it is possible that some of the issues in this appeal may have fallen away.

496. The suggestion that the time period for compliance with the corrective orders is too short is little more than a bald assertion by TikTok and is unsupported by evidence. The issue is addressed at §568 to §578 of the affidavit of Elaine Fox, but her evidence is no more than an assertion that the timeframe is “*wholly unrealistic*”. The context for the timeframe is the DPC’s conclusion that TikTok has infringed Article 46 by transferring personal data to China without first having ensured that equivalent protection to that available within the EEA was guaranteed and that that shortcoming had not been addressed. Far from being obliged in those circumstances to afford TikTok a generous period within which to re-organise its affairs or address those failings, the DPC acted well within its margin of discretion by affording a reasonable period within which transfers in the absence of an adequate assessment were required to stop. TikTok has not identified any error in its so doing. There is no inherent impossibility of compliance as in *Lawlor*.

497. I note as an aside that TikTok’s evidence in the stay application tends to undermine its contention in this appeal that compliance with the corrective orders within six months was unachievable. It may be, as the evidence there showed, that compliance is unduly onerous for TikTok, but as I concluded in that judgment, TikTok cannot rely on the manner in which it structures its business to justify an entitlement to carry on that business without complying with the GDPR (at §216 of the stay judgment).

Overall conclusion on Ground 11

498. TikTok has not identified any stand-alone ground of appeal by reference to the manner in which the DPC made the corrective orders.

499. The DPC correctly considered whether corrective orders were appropriate and proportionate in the circumstances of this case. In particular, it considered whether there was any change between the finding of the infringement and the decision to make corrective orders which meant that corrective orders were unnecessary. Having regard to the DPC’s conclusions on those issues, the DPC’s decision that a suspension order rather than a request

to submit a further DTA was the least onerous means of securing the objectives of the GDPR was entirely justified.

500. The corrective orders were neither vague nor impossible to comply with.

Ground 5 – misrepresentation and misapplication of Article 13(1)(f)

501. This is the only ground challenging the finding of infringement in relation to Article 13(1)(f) of the GDPR. Article 13(1) imposes transparency requirements on controllers of personal data. It requires that controllers inform data subjects that it is intended to transfer their personal data to a third country and to refer to the appropriate or suitable safeguards which are in place.

502. The adverse finding relates to TikTok’s 2021 Privacy Policy, the DPC having concluded that TikTok’s updated 2022 Privacy Policy complied with the requirements of Article 13(1)(f). The relevant wording of the 2021 Privacy Policy is as follows:

To support our global operations, we share your information with members of our Corporate Group and other entities outside of your country of residence as described in the “How We Share Your Information” section. These entities are committed to using and storing information in compliance with applicable privacy laws and to implementing appropriate security measures to protect your information.

When we transfer your information outside of the European Economic Area (EEA), the United Kingdom, or Switzerland, we ensure it benefits from an adequate level of data protection by:

- relying on European Commission adequacy decisions made under Article 45 of the GDPR, finding that the third country to which the information is being transferred offers an adequate level of data protection; or*
- using European Commission approved standard contractual clauses under Article 46 of the GDPR for the transfer of information to all other third*

countries. For a copy of these standard contractual clauses, please contact us via the details provided in the “Contact us” section below.

503. As appears from the foregoing, the policy did not expressly reference any third country to which data was being transferred, in particular, China. Nor was there any explanation of the nature of processing operations. The DPC concluded that both were required by Article 13(1)(f) and therefore the GDPR had been infringed (at §592 – 595):

First, the DPC finds that the October 2021 EEA Privacy Policy should have informed EEA Users of the named third countries, including China, to which personal data was transferred, and did not do so. The DPC does not agree with TikTok Ireland’s submission that it was not necessary, under Article 13(1)(f) GDPR, for TikTok Ireland to name the third countries to which personal data is transferred using SCCs. The DPC considers that it is clear from the text and the context of Article 13(1)(f) GDPR that this information ought to have been provided in the circumstances of the Data Transfers. Where Article 13(1)(f) GDPR requires controllers to inform data subjects of whether, for example, personal data is transferred in reliance on an adequacy decision, or SCCs, or derogations under Article 49 GDPR, it is part of the necessary context for that information regarding the transfer mechanism for that information to be linked to the named third country in respect of which the transfer mechanism is being used. In this regard, the wording of Article 13(1)(f) GDPR makes express reference to “a third country or international organisation”, rather than to a destination “outside of the EU”. The specific third country or international organisation to which the data is transferred is of obvious relevance to allow the data subject to know how and where their personal data is processed, and, indeed, to verify at a very basic level that an appropriate transfer mechanism is in place. This follows from the need, highlighted in recital 39 GDPR, for data subject “to be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing”. This concern is further highlighted by the Article 29 Working Party as follows:

A central consideration of the principle of transparency [...] is that the data subject should be able to determine in advance what the scope and consequences

of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used.

Having regard to the above, the DPC agrees with the view adopted by the Article 29 Working Party that for information provided under Article 13(1)(f) to be meaningful, it must specify the named third countries to which the personal data of EEA users is transferred unless this information is already available to data subjects, for example, by reference to an adequacy decision relied upon. In this case, the DPC finds that the October 2021 EEA Privacy Policy should have specified each of the third countries to which EEA User Data was transferred by TikTok Ireland, including China.

Second, in circumstances where the concept of a “transfer” of personal data is not expressly defined in the GDPR, and is capable, in this context, of consisting of more than one single type of processing operation, the DPC finds that the information required under Article 13(1)(f) GDPR included an explanation, using clear and plain language, of the nature of the processing operations that constitute the transfer.

In this case, during the temporal scope, the processing concerned was remote access to personal data stored in Singapore and the United States by personnel of the China Group Entities based in China. The DPC considers that in order for the processing of personal data to be fair and transparent in light of the obligations on TikTok Ireland under Article 13(1)(f) read with Article 12(1) GDPR, a basic factual description of the transfers should have been made available to EEA Users in the October 2021 EEA Privacy Policy. The DPC considers, in this regard, recalling recital 60 GDPR, that this information is “necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed.”

504. For comparison, the relevant portion of the 2022 Privacy Policy is as follows:

Our Global Operations and Data Transfers: Storage and Limited Remote Access within our Corporate Group We explain below how EEA/UK user information benefits from an adequate level of protection when certain entities in our Corporate Group provide necessary services to support our Platform.

Storage

We provide our Corporate Group entities located in the United States and Singapore with the information described in What Information We Collect under standard contractual clauses so that they can store it for us on secure servers.

Limited Remote Access

Adequacy decisions. Certain entities in our Corporate Group located in Canada, UK, Israel, Japan and South Korea are granted limited remote access to information described in What Information We Collect to provide important functions. We rely on the European Commission adequacy decisions (or equivalent decisions under other laws) to grant these entities remote access.

Standard contractual clauses. Certain entities in our Corporate Group located in countries without an adequacy decision are granted, under standard contractual clauses, limited remote access to information described in What Information We Collect to provide important functions. These entities are located in Brazil, China, Malaysia, Philippines, Singapore, and United States.

Arguments

505. Both parties rested on their written submissions. TikTok identify a number of alleged errors in the DPC's analysis. First, it observes that Article 13(1)(f) does not expressly state that the third country to which data is being transferred must be identified, or that the nature of the processing be explained, and that the DPC has, therefore, imposed obligations which "[go] beyond the requirements of the text". It argues that the DPC's interpretation is inconsistent with the text of Article 13(1)(f), "*the context in which it occurs, and its objectives*". It also contends that the requirements contended for by the DPC are inconsistent with the requirement in Article 12(1) that information provided under Article 13 be in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language.*"

506. It contends that the DPC erred by reading Article 13(1)(f) in light of Article 15(1)(c), which confers on data subjects a right of access to information on recipients of personal data, in particular recipients in third countries, which TikTok contends “*operated in a different context*” to Article 13.

507. TikTok argues that the DPC’s reliance on the Working Party Guidelines on Transparency under Regulation 2016/679 was misplaced as they are non-binding guidelines and, in any event, do not require the nature of the processing to be explained.

508. Finally, TikTok contends that the DPC’s “*expansive*” interpretation of Article 13(1)(f) is not in accordance with the requirements of legal certainty and that provisions giving rise to potential penal sanctions should be strictly construed.

509. The DPC argues that the requirement to identify the third country to which data was being transferred arose in this case in order to meet the requirements of transparency. It argues that this is consistent with the requirement in Article 13(1)(f) to indicate whether or not there is an adequacy decision – which necessarily presupposes identifying the country to which the adequacy decision relates. It is also argued to be consistent with the necessity to provide the identity of the recipients of data (see Article 13(1)(e)).

510. The DPC argues that its interpretation is consistent with a teleological interpretation of the GDPR, necessary to ensure transparency and a high level of protection for personal data.

511. In relation to the requirements for a description of the type of processing, it contends that its reading of the requirements of Article 13(1)(f) is consistent with Article 13(2) which indicates that the purpose of providing information is to ensure “*fair and transparent processing*”. The DPC also relies on Recital 60 which refers to the “*specific circumstances and context in which the personal data are processed*”. It suggests that the requirement that the data subjects be informed of the appropriate safeguards imports a requirement to be told the nature of the processing. It refers to *The EU General Data Protection Regulation (GDPR): A Commentary* (ed. Kuner et al, Oxford University Press, 2020) at p. 416 which notes, in relation to Article 13, that as “*far back as the 1980s, the right to information about the processing operation was called ‘chief’ among the rights of the data subject*”.

512. The DPC argues that there is no inconsistency with Article 12(1) and no error in having regard to Article 15(1). Nor, it says, is there any breach of the requirement for legal certainty.

Discussion

513. It is clear from Article 12 of the GDPR that the purpose of providing the information specified in Article 13(1) is to ensure fairness and transparency in order to enable data subjects to exercise their rights under the GDPR. The provisions of Article 13(1), therefore, fall to be interpreted as requiring the provision of the information which is sufficiently fair and transparent to enable data subjects to exercise their rights.

514. On a plain reading of Article 13(1)(f), the obligation imposed is *capable* of being interpreted as being confined to being an obligation merely to advise of the fact that data is being transferred to a third country or international organisation, as the DPC seems to have accepted. Such a reading is plausible, however, only if one disregards the purpose of providing the information. When one considers that the information is required to enable data subjects to exercise their rights, it is apparent, that those data subjects will, in almost all cases, be required to be told to which country the data is being sent. The Working Party Guidelines on Transparency suggests that in the interest of fairness, it will “*generally*” be necessary to name the third country to which data is being transferred. In fact, it is difficult to imagine any circumstance in which advising data subjects that their personal data had been transferred to a third country without telling them what that country is could meet the requirements of fairness or transparency. Where transfers to a third country are regulated by an adequacy decision, there is an express requirement that the data subject is told. Unless the data subjects are told which adequacy decision is being relied on, then the data subject is not adequately informed about the transfer: the data subjects must necessarily, therefore, be advised of what countries data is being transferred to on the basis of adequacy decisions. If that is so, it is almost inconceivable that they need not also be told of which third countries to which data is being sent that do *not* have the benefit of adequacy decisions.

515. Where data is transferred to a third country, it is required to be subject to an equivalent level of protection to that guaranteed within the EU. Data subjects would be deprived of their ability to consider for themselves whether their data is, in fact, afforded the requisite level of protection, and to exercise their rights accordingly, if not adequately informed of

the countries to which their data is transferred. A data subject must be entitled to raise with a supervising authority the question of whether their data is adequately protected. Data subjects' rights would be seriously undermined if a controller could continue transferring personal data without even identifying to those data subjects to what country that data was being sent.

516. Though I think it must almost always be necessary to identify the third country to which data is being transferred, Article 13(1)(f) can also properly be interpreted as imposing a requirement to provide an indication of the nature of processing involved where that is necessary to ensure fairness and transparency. Such an obligation may arise having regard to the necessity to identify the appropriate or suitable safeguards. It seems to me that the DPC were correct to conclude that this is a case in which that obligation arose. As is apparent from the discussion above, the fact that personal data was only remotely accessed, and was stored outside China, was at the heart of TikTok's argument that equivalent protection was afforded to personal data transferred to China. The 2021 Privacy Policy in no way identified the fundamental protection relied on by TikTok, or afforded data subjects a fair opportunity to consider the nature of what TikTok was doing. Of course, since TikTok did not indicate that it was transferring data to China at all, an explanation of the nature of those transfers didn't arise. Had it advised data subjects that data was being transferred to China, then, on TikTok's case, it was in *TikTok's* interests that data subjects be made aware that personal data was subject only to remote access, and was stored outside China, since this would have highlighted the principle basis relied on by TikTok for asserting that those transfers were GDPR compliant. That TikTok failed to advise its users of information which it was in TikTok's interest to share is not a basis for concluding that its Privacy Policy was compliant.

517. The requirement to identify third countries to which data is being transferred and to give an indication of the nature of the processing is also entirely consistent with Recital 60 of the GDPR.

518. As the 2022 Privacy Policy amply demonstrates, this information could readily be provided in clear language. TikTok's argument regarding inconsistency with Article 12 is without foundation.

519. The complaint about reliance on Article 15(1)(c) of the GDPR does not assist TikTok. As made clear above, the GDPR must be read as a whole, and as internally consistent. There is no error in having regard to other provisions of the GDPR when interpreting any particular provision. In any event, the requirement to identify recipients of data contained in Article 15(1)(c) is also to be found in Article 13(1)(e). TikTok could not sensibly argue that it was inappropriate to consider the provisions of Article 13(1)(e) when seeking to understand the scope of the obligation imposed by Article 13(1)(f).

520. No basis for arguing that the provisions of Article 13(1)(f) fail to meet the obligations of legal certainty was identified: it was merely asserted by TikTok. Article 13(1)(f) imposes obligations which must satisfy the requirements of fairness and transparency. There is nothing opaque or uncertain about what was required, and the 2021 Privacy Policy fell short of what was necessary.

521. In light of the foregoing, the DPC's conclusion that the 2021 Privacy Policy did not comply with Article 13(1)(f) of the GDPR was manifestly correct. It could not plausibly have reached any other conclusion than that, in the circumstances of the transfers the subject of these proceedings, the privacy policy was required to identify the third countries to which data was being transferred. The finding in relation to the requirement to indicate the nature of the processing was also, in the particular circumstances of this case, correct.

522. In circumstances where TikTok has invited the court to substitute its view for that of the DPC, I would add further that the 2021 Privacy Policy is, in my view, inadequate in two further respects. First, there is a failure to expressly indicate to which countries data is transferred in reliance on adequacy decisions, or those to which data is transferred, like China, in the absence of an adequacy decision. Article 13(1)(f) expressly requires that the existence or absence of an adequacy decision be identified. The 2021 Privacy Policy does not identify any country or adequacy decision relied on. At no point does it expressly state that data is transferred to countries with no adequacy decision, still less which countries those are. True, the policy does refer to data being transferred either on the basis of adequacy decisions or standard contractual clauses, but the Policy completely fails to meet the obligations of fairness and transparency in this respect.

523. Secondly, the suggestion that data is transferred on the basis of standard contractual clauses is simply inaccurate. In the case of China at least, TikTok accepts that the standard contractual clauses alone do not provide sufficient protection for the data transferred. This last statement, which I note remains in the 2022 Privacy Policy, is, therefore, positively misleading. Although I was told by TikTok in oral submissions that this was “*commonplace in privacy policies*” (Transcript Day 4, page 122), this does not excuse the shortcomings in TikTok’s transparency obligations.

Overall conclusion on Ground 5

524. TikTok has not established any error by the DPC in concluding that TikTok was required to identify the third countries to which data was being transferred in its privacy policy and to set out the nature of the processing involved.

525. In the circumstances, I reject TikTok’s fifth ground of appeal and, accordingly, confirm the finding that TikTok’s 2021 Privacy Policy infringed Article 13(1)(f) of the GDPR.

Appeal against fines

526. The conclusions above regarding errors in the assessment of whether to make a corrective order have no bearing on my conclusion that the DPC was entitled to make the findings of infringement which it did, and my rejection of all the grounds of appeal impugning those findings. Accordingly, those conclusions have no bearing on TikTok’s appeal against the fines imposed for those infringements.

527. TikTok make a number of complaints about the decision to impose administrative fines and the manner in which the DPC calculated those fines. By way of summary only, TikTok contends:

- The DPC was only entitled to impose a fine if it concluded that TikTok’s infringement was negligent or intentional and it failed to establish that TikTok was negligent (Ground 6);

- The DPC impermissibly had regard to the turnover of ByteDance in determining the fining caps and the amount of the actual fines (Ground 7);
- The DPC failed to provide adequate reasons for the fining decision (Ground 8); and
- The DPC made errors of fact in its interpretation and application of Article 83 (Ground 9).

528.As noted, the parties have requested that I refer various questions to the CJEU pursuant to Article 267 of the TFEU on issues arising from TikTok’s grounds of appeal. A reference to the CJEU could only arise if a question of EU law is raised in the proceedings and a decision on that question is necessary to enable the court to give judgment. The first ground of appeal against the decision to impose administrative fines disputes the DPC’s conclusion that it was entitled to impose fines at all because there was no basis for its finding of negligence. This is not an issue in the annulment proceedings, *WhatsApp v EDPB*.

529.If TikTok is correct that the necessary elements for a finding of negligence were not present, then no fine could properly have been imposed and none of the other issues arise. A decision on them would not then be “*necessary*” to enable me to deliver judgment. In those circumstances, it seems to me to be convenient to deal with that threshold question first, before, if necessary, returning to deal with the other grounds of appeal. I should note that the parties have agreed a formulation of three questions addressing this issue for potential referral to the CJEU. For the reasons set out below, I do not consider that a referral on those questions is necessary or would be appropriate.

Ground 6 – failure by the DPC to establish that TikTok was negligent

530.Article 83(2) of the GDPR sets out the factors to which regard must be had by a supervising authority when deciding whether to impose an administrative fine. Article 83(2)(b) identifies the “*the intentional or negligent character of the infringement*” as one such factor. The parties agree that a supervising authority is not entitled to impose administrative fines under the GDPR in the absence of a finding of fault, either negligence or intention, on the part of the data controller or processor. This was not always apparent but was confirmed in two cases decided at the same time, *NVSC*, referenced above, and Case C-807/21, *Deutsche Wohnen*.

531. The test for negligence is that which applies in the competition law sphere. As expressed in *Deutsche Wohnen* (at §76):

“In that regard, it must be clarified, as regards the question whether an infringement has been committed intentionally or negligently and is, therefore, liable to be penalised by an administrative fine pursuant to Article 83 of the GDPR, that a controller can be penalised for conduct falling within the scope of the GDPR where that controller could not be unaware of the infringing nature of its conduct, whether or not it is aware that it is infringing the provisions of the GDPR.”

532. The formulation is, at first glance, a little difficult to understand, but if “*could not be unaware*” is framed without the double negative, then the threshold for negligence (or intentionality) can readily be understood as a controller being liable, whether or not it knew it was infringing the GDPR if it could have been aware that its conduct was infringing. Put otherwise, an infringement is not negligent or intentional if a controller could not have been aware of the infringing nature of the conduct.

533. Thus framed, it is apparent that the threshold is a low one. This is reflected in the observations of the Advocate General in *NVSC* (at §80) :

“Fourth, and perhaps most importantly, I consider that, in practice, the threshold for a negligent infringement of the GDPR, within the meaning of Article 83(2)(b) of that regulation, is, in any case, so low that it is difficult to envisage situations where it will be impossible to impose a fine for the mere reason that that element is not satisfied.”

534. A slightly different standard was at issue in a case on which TikTok relied in its submissions to the DPC, Case C-308/06, *Intertanko*. The relevant portion of the judgment relates to Article 4 of Directive 2005/35 which obliges states to punish ship-source discharges of polluting substances if committed “*with intent, recklessly or by serious negligence*”. The Court pointed out (at §73) that:

“It is, however, to be pointed out, first of all, that those various concepts, in particular that of ‘serious negligence’ referred to by the national court’s questions, correspond to

tests for the incurring of liability which are to apply to an indeterminate number of situations that it is impossible to envisage in advance and not to specific conduct capable of being set out in detail in a legislative measure, of Community or of national law.”

535. Noting that the concepts were “*fully integrated into*” the Member States’ legal systems, the Court stated (at §75 and §76):

“In particular, all those systems have recourse to the concept of negligence which refers to an unintentional act or omission by which the person responsible breaches his duty of care.

Also, as provided by many national legal systems, the concept of ‘serious’ negligence can only refer to a patent breach of such a duty of care.”

536. In the PDD, the DPC provisionally concluded that the infringements were negligent (see §479 - §486). In the response to the PDD, TikTok identified a series of facts which it said showed that it was not negligent. Some of these facts amounted to claiming that it had not infringed at all, but those directed to its level of fault included that it had prepared detailed DTAs, and had confirmed its position in relation to Chinese law from a number of experts, including Fangda Partners, Clifford Chance and Professor Xu, that this was a “*complicated area of law*” as evidenced by the Milieu report. It characterised the PDD findings as being that matters were insufficiently explained, and stated that there were no “*errors of assessment*”. It noted its significant investment in the development of new supplementary measures.

537. The DPC assessed Article 83(2)(b) at §738 to §748 of the Decision. It noted that the GDPR does not identify the factors which need to be present for an infringement to be classified as ‘intentional’ or ‘negligent’, but referred to the WP29 Guidelines on the application and setting of administrative fines for the purpose of Regulation 2016/679 (“**the Administrative Fines Guidelines**”) which provide:

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

538. The Administrative Fines Guidelines, the Decision records, provide that conclusions on intent or negligence will be drawn on the basis of identifying objective elements of conduct from the facts of the case. At §741, the DPC characterised the test as whether the objective elements demonstrate that the controller “*ought to have been aware*” that it was falling short of the duty owed.

539. The DPC concluded (at §742) that although TikTok had wilfully transferred data, it did not *know* that it had failed to verify. Intent was not, therefore, made out. It concluded that TikTok was negligent to “*a high degree*” because it ought to have been aware of the flaws in its DTAs. The fact that it had carried out the DTAs did not mean that it was not negligent. The DPC also concluded that TikTok was negligent in relation to the Article 13(1)(f) infringement.

Arguments

540. In their submissions, TikTok complains that the DPC does not reference the decisions in *NVSC* and *Deutsche Wohnen* in the Decision and implicitly criticise its reliance instead on the Administrative Fines Guidelines. It identifies the following purported errors by the DPC:

- The DPC failed to recognise that the identification of negligence was a threshold issue and does not flow automatically from an infringement;
- It failed to identify the standard of care;
- It failed to find any objective basis for the finding of negligence and ignored evidence inconsistent with negligence;
- It failed to provide adequate reasons supported by evidence.

541. In oral submissions, it was suggested that the test set out in the Administrative Fines Guidelines was not the same as the *NSVC* and *Deutsche Wohnen* tests and that on one reading the Guidelines could be read as saying “*if you have infringed, that’s enough*” (Transcript, Day 5, p. 84). In articulating the threshold TikTok said that there must have been some deficiency of which the controller ought to have been aware.

542. Counsel focused on the finding of negligence at §742 of the Decision. She characterised it as saying nothing more than a conclusion without explanation, failing to identify the flaws or why TikTok should have been aware of them. She makes similar criticisms of the conclusion in relation to Article 13(1)(f).

543. The DPC point out that the Decision does, in fact, acknowledge that negligence (or intention) finding is a prerequisite to a decision to impose an administrative fine and does reference the judgment in *NVSC* (at §810). It emphasises that the standard for establishing negligence is low. It says that it hasn’t ignored any of TikTok’s evidence as to why it wasn’t negligent and that it has met the standard identified in *Connelly v An Bord Pleanála* [2021] 2 IR 752, in giving, as it puts it, the “*main reasons on the main issues*”. In oral submissions, it stresses that its findings in relation to negligence must be read in the context of the Decision as a whole and, in particular, the DPC’s conclusion that TikTok had not adequately assessed the data transfers the subject of the Inquiry.

544. It draws comparisons with the decisions of the CJEU referenced in *Deutsche Wohnen* and *NVSC* which contain the test for negligence quoted above, including Case C-681/11, *Schenker*, Case C-591/16P, *Lundbeck*, and Case C-601/16P, *Arrow Group*.

Discussion

545. I do not consider that there was any error by the DPC in concluding that TikTok was negligent in infringing Articles 46 and 13(1)(f). Even if there were some error by the DPC in the manner it reached or expressed that conclusion, in an appeal on the record, I would not substitute any other conclusion for that of the DPC. TikTok was negligent in committing the infringements of the GDPR.

546. Subtending TikTok's assertion that there was no basis for a finding of negligence is its contention that it discharged its obligations by preparing detailed DTAs, which comprehensively addressed the risks to personal data. TikTok is a major data controller, seeking to transfer very significant amounts of data from the EEA to a third country. The fact that it carried out detailed assessments to enable it to transfer data to China does not of itself discharge its duties under the GDPR. I have concluded above that the DPC was entitled to conclude that, despite TikTok's efforts, those assessments were inadequate, *i.e.* that there was a falling short by TikTok. So the question is not, as TikTok appears to consider, did TikTok *attempt* to discharge its duty, or did it make significant efforts to discharge its duty. Rather, it is whether its failure to do so can be attributed to any fault on TikTok's part. However the negligence threshold in the GDPR is calibrated, it is clear that it was at fault.

547. TikTok criticise the DPC for failing to identify the standard of care. The DPC say that it wasn't required to do so, but the better point is that it did so throughout the Decision (and the PDD) in identifying where TikTok had fallen short. The standard to be met is that set out *Schrems II*, to verify that effectively equivalent protection to that available in the EEA is guaranteed. The issue to be considered in determining intent or negligence was the level of fault.

548. The threshold is articulated in *Deutsche Wohnen* and *NVSC*. Could the controller not have been unaware that its conduct was infringing? Could it have been aware that its conduct was infringing? On any view, that is a low threshold, as identified by the Advocate General in *NVSC*. At the hearing, TikTok contended for a threshold of whether it "*ought to have known*", which, arguably is higher than that identified in the case law. As noted, that is the standard which the DPC purported to apply (see §741 of the Decision). But even taking that as the standard, the answer in my view is that, yes, it ought to have known. Indeed, no other conclusion is possible from TikTok's own evidence. How could it not have known that it was required to assess the level of protection afforded to personal data transferred to and being processed in China? As is apparent from the decision in *Schenker*, the fact that TikTok may have engaged experienced lawyers to advise it on whether its conduct was in accordance with the requirements of the GDPR does not relieve it of liability.

549. As noted above, the focus of Chapter V of the GDPR and, necessarily, the Inquiry is on personal data transferred to third countries for processing: thus, in this case, the personal

data transferred by TikTok to China by remote access for processing. The question to be addressed is what level of protection that data was given as a matter of Chinese law. As appears from the analysis above, the protection afforded to locally processed data was not directly addressed by TikTok until the third Xu opinion. TikTok's case, at its height, is that it was *implicitly* addressed in Professor Xu's second opinion, supplied in September 2023, *i.e.* after the temporal scope of the Inquiry, and expressly addressed in the July 2024 DTA.

550. TikTok does not argue that the local processing issue did not *have* to be addressed as part of the verification process prior to transferring data. Its main complaint is that it did not know that was the (or a) concern of the DPC and would have addressed it had it known. It has provided no explanation for its failure to do so prior to, on its case, the second Xu opinion (though this was only stated in the third Xu opinion). It does not identify any other evidence where it says local processing was addressed, or even identified as an issue.

551. If TikTok had been correct that, because local processing was inevitable, it must be taken to have addressed that processing in its DTAs' conclusions that the remote storage of data (with other measures) guaranteed equivalent protection, then it might be able to argue that its 'fault' was no more than it failed to express that which was obvious. But even if that proposition was not built on faulty logic, it is at odds with TikTok's own evidence, contained in the third Xu opinion, that the locally processed data is afforded the necessary protection by the application of Chinese laws which treat it as overseas data and, therefore, of the same status as the data permanently stored overseas.

552. It is important to emphasise here that TikTok's complaint that the Inquiry didn't make clear that the local processing issue was a particular concern is not relevant to the question of whether TikTok was negligent. If the issue required to be addressed before data was transferred, and as I have made clear above, it is the issue which should have been the focus of any data transfer assessment by TikTok, then TikTok cannot avoid a conclusion of negligence by suggesting that the Inquiry process did not highlight this falling short. And the fact that TikTok did not *actually* know that it had not addressed an issue which required to be addressed is not an answer either. If it did know, then that would render the infringement intentional.

553. TikTok, accordingly, failed to verify that the locally processed data was subject to essentially equivalent protection during the temporal scope. It does not argue that this was

not an issue which required to be addressed prior to transferring data. This was, in fact, the most obvious issue which required to be addressed. It provides no explanation for its failure to do so. The first evidence it relies on to suggest that it *was* addressed post-dates the temporal scope (the second Xu opinion). Its subsequent evidence (the third Xu opinion) undermines that contention. Though TikTok trumpets the efforts it went to carry out its data transfer assessments, and the measures that it put in place, it does not, when properly analysed, proffer any argument that the requirement to assess the locally processed data was not something it *ought* to have known, still less that it was something that it *could not* have known should be addressed.

554. On the application of the test articulated in the CJEU authorities, TikTok could not have been unaware that it was required to assess the local processing issue and, therefore, was not permitted to transfer prior to so doing, *i.e.* that its conduct was infringing. It is the express and obvious obligation imposed by Chapter V of the GDPR. By transferring large amounts of data without carrying out that assessment, TikTok was clearly negligent.

555. TikTok does, at least, have an *argument* that it could not have been unaware that its 2021 Privacy Policy was not in breach of Article 13(1)(f) of the GDPR because the requirement to tell data subjects that their data will be transferred to a third country does not impose an *express* obligation to identify that country. However, as I have concluded above, that is what the GDPR and its transparency obligations, properly interpreted, *does* require, certainly in the circumstances of this case. TikTok cannot rely on a misunderstanding of its obligations to excuse a failure to comply with them, certainly not in the absence of any evidence of the efforts it went to understand those obligations.

Overall conclusion on Ground 6

556. There was no error by the DPC in its conclusion that TikTok was negligent in infringing both Article 46 and Article 13(1)(f) of the GDPR.

557. TikTok failed to comply with an obvious obligation under Article 46, with no explanation for such failure, and failed to understand its obligations under Article 13(1)(f), but has not identified any reason to justify its misunderstanding. In those circumstances, no

conclusion other than that TikTok was negligent was open to the DPC and there is no basis upon which the court could set aside its conclusion on this issue. Even had DPC erred in its assessment of the question of whether TikTok had been negligent, on the evidence available, there is no basis to interfere with its conclusion that it had been.

558. In the particular factual circumstances of this case, there is no legal uncertainty about this conclusion such that a reference to the CJEU might be required.

Summary of conclusions

559. As confirmed in *LinkedIn v DPC*, the appeal provided for in both sections 142 and 150 of the 2018 Act is an appeal on the record. In such an appeal, the court is entitled to consider all the evidence which was before the DPC on its merits, and any additional evidence which may be admitted. Where an error is identified in the DPC's decision, the court is entitled to substitute its own order for that of the DPC where it considers this appropriate. In assessing the evidence of the DPC, the court should afford deference to its views on matters falling within the sphere of its expertise.

560. Having regard to the very significant fines which may be imposed for infringements of the GDPR, the sanctions should be considered punitive or criminal in nature such that the rights of the defence protected by Article 48 of the Charter and Article 6 of the ECHR are engaged.

561. There was no error of law by the DPC in its interpretation and application of the GDPR. The GDPR places an obligation on controllers to verify that the level of protection afforded to personal data transferred to third countries is essentially equivalent to that guaranteed within the EEA. Where controllers transfer data to third countries they must be in a position to demonstrate when called upon to do so that they have adequately verified the level of protection. A supervisory authority is entitled to assess the adequacy of a controller's verification in order to determine whether it has complied with the GDPR and find an infringement where the verification is not adequate.

562. This is consistent with the principles of accountability in Articles 5 and 24 of the GDPR and the decision of the CJEU in *Schrems II*.

563. There was no impermissible reversal of the burden of proof by the DPC in finding an infringement of Article 46 of the GDPR. Having regard to its conclusion that TikTok had not adequately assessed the level of protection afforded to personal data transferred to China, there was no error by the DPC in its approach to the risk of such transfers. The DPC considered whether a suspension order was necessary, appropriate and proportionate.

564. There was no breach of fair procedures by the DPC when concluding that TikTok had failed to assess the level of protection afforded to data being processed in China. That issue was at the heart of the Inquiry and was central to TikTok's obligations under Article 46. TikTok had more than sufficient notice that this was an issue which it was required to address and more than adequate opportunity to address it.

565. There was no breach of fair procedures in fixing the temporal scope of the Inquiry, or at least no breach independent of its complaint that material submitted after the temporal scope was not adequately considered. The DPC could not, by limiting the temporal scope of the Inquiry, gives less consideration to material submitted during the Inquiry outside the temporal scope, to which it had agreed to have regard.

566. No breach of fair procedures has been identified by reason of the DPC's refusal to provide very limited material to TikTok concerning its interactions with other SACs. TikTok had no entitlement to that material and, even if it did, has failed to show that there was anything in the material which had a bearing on its rights of defence.

567. There was no error by the DPC in its assessment of TikTok's evidence regarding the relevant Chinese laws up to the delivery by TikTok of the third Xu opinion. The DPC's conclusion that the evidence did not address the level of protection afforded to personal data transferred to and being processed in China was amply supported by the evidence. There was, accordingly, no breach of fair procedures by the DPC in failing to engage with footnote 113 of the July 2024 DTA in the Decision.

568. Having regard to the necessity to balance the rights of the defence with the obligation to complete inquiries within a reasonable time and with due diligence, the DPC would have been entitled to fix a time beyond which no further material from TikTok would be accepted or considered. It did not do so. In circumstances where the DPC had not fixed a time beyond

which further material would not be considered, and where it, in fact, accepted and considered material submitted at an even later date, in the very particular circumstances of this case, fair procedures required that the DPC have regard to the third Xu opinion to the extent that it was relevant to the issues in the Inquiry, and in particular, to the question of whether to make a suspension order.

569. The third Xu opinion is, on its face, relevant to the question of whether a suspension order was necessary, appropriate and proportionate. In circumstances where the DPC did not have regard to the opinion, the court is required to have regard to it when considering whether to substitute any order for the suspension order made by the DPC.

570. The DPC had regard to the Project Clover measures implemented by TikTok after the temporal scope and, as it was entitled to in the exercise of its technical expertise, concluded that a suspension order was still warranted. In the ordinary course, the court would defer to the DPC's expertise on this matter. However, in breach of fair procedures, the DPC has failed to give any or any adequate explanation for the apparent rejection of the adequacy of the measures introduced by TikTok.

571. The Project Clover measures are clearly relevant to the question of whether a suspension order was necessitated in this case. The court is required to have regard to those measures in considering TikTok's appeal against the suspension order and whether to substitute an alternative order. In the absence of any reasons having been given by the DPC for rejecting the measures, it is not possible to afford deference to the exercise by it of its technical expertise when assessing this evidence.

572. There was no error of law by the DPC in its approach to the making of the corrective orders. It was not required to make a further finding of infringement before so doing, it was not required to instead request a further DTA from TikTok, there was no vagueness or ambiguity in the processing order and the time given for compliance with the corrective orders has not been shown to be unreasonably short.

573. No error of law or fact has been identified by TikTok in relation to the DPC's conclusion that TikTok's 2021 Privacy Policy breached Article 13(1)(f) of the GDPR. Consistent with the obligation of transparency, TikTok was required to identify in that policy the countries

to which it was transferring data. It was also required to identify the nature of the processing involved. It failed to do so.

574. There was no error by the DPC in concluding that TikTok's infringements of Article 46 and Article 13(1)(f) were negligent in character. Those conclusions were amply supported by the evidence. The DPC was thus entitled to impose administrative fines for those infringements.

Proposed Order

575. As noted at the outset, the Decision had four component parts: the finding of infringement of Article 46; the finding of infringement of Article 13(1)(f); the decision to impose administrative fines for those infringements; and the decision to impose the corrective orders in light of the finding of infringement of Article 46.

576. I have rejected above all the grounds of appeal directed at the first two components of the Decision, the infringement findings. I propose, therefore, to dismiss all the grounds of appeal against those infringement findings.

577. I have, in addition, concluded that there was no error by the DPC in concluding that both infringements were negligent in character within the meaning of Article 83(2)(b) of the GDPR and that that necessary prerequisite to the imposition of an administrative fine was met. I propose accordingly to dismiss the appeal against the decision to impose administrative fines. For the reasons explained above, I will leave over for further decision TikTok's appeal against the *amount* of the fines imposed.

578. Although I have concluded that there was no error of law by the DPC in the approach it took to the question of whether to impose corrective orders, I have also concluded that there were errors in its actual assessment of the information relevant to the question of whether to impose, in particular, the suspension order.

579. I have rejected the contention by TikTok that an identification of *any* error by it automatically leads to the annulment of the Decision (or part of it). This is not consistent with a statutory scheme in which the court is entitled to consider the merits of the DPC's

decision, hear new evidence and substitute its own requirements in place of those required by the DPC. The role of the court is to attempt, if possible, to determine the appropriate order in light of the evidence. The fact that there may have been errors of assessment by the DPC does not lead to the inevitable consequence that its ultimate conclusion was in error.

580. This is consistent with the case law of the CJEU. In Case C-297/23P, *Harley Davidson Europe Ltd* concerned an appeal against the revocation of binding origin information (BOI) decisions relating to the importation of motorcycles. The General Court, despite finding that the Commission had erred by failing to hear from the appellant before adopting its decision, concluded that that was not sufficient to result in the annulment of the decision. The CJEU concluded that there was no error by the General Court in so doing (at §104):

“Second, in order to have a contested measure annulled on the basis of Article 263 TFEU, it is for the person alleging an infringement of his or her rights of defence to show that there is a possibility that the administrative procedure leading to the adoption of that measure might have led to a different outcome ... In that regard, although a person who relies on such an irregularity cannot be required to show that, in its absence, the act concerned would have been more favourable to his or her interests, he or she must nevertheless prove, in a concrete manner, that such a possibility is not entirely excluded ...”

581. Although TikTok has succeeded in establishing errors in the DPC’s assessment, it is not clear to me at this juncture that it has established that a different form of order than that imposed by the DPC is appropriate.

582. It is necessary to consider the two identified errors of assessment in turn, but also together.

583. The first error concerns the consideration of the third Xu opinion. As noted, there is some ambiguity about how the DPC dealt with this opinion, it either disregarded it entirely, or it considered that it was not material to the issues of concern that it had raised and therefore did not need to be addressed. Whichever of those views it took, it was in my view in error. Although the opinion was submitted very late in the day, for the reasons explained, it should not have been disregarded for that reason alone.

584. Once the opinion is considered, it does at least raise the possibility that TikTok had, belatedly, adequately assessed the level of protection afforded to personal data being processed in China, clearly a relevant consideration in determining whether a suspension order was appropriate, necessary and proportionate.

585. Though the DPC did not consider that possibility, the court can or can attempt to do so. I have some doubt about whether the third Xu opinion could, by itself, be regarded as discharging TikTok's obligation to verify that equivalent protection to that available in the EEA was guaranteed for the data transferred, and for that purpose to carry out an adequate assessment of the protection available. Though Professor Xu does conclude that equivalent protection is guaranteed, his reasons for doing so appear somewhat speculative. It is a bold conclusion based on apparently slim legal foundations. Given the centrality of the issue to the Inquiry, the DPC could not have been obliged to simply accept Professor Xu's conclusion on its face, especially where it appears to represent a departure from his second opinion, or at least a different analysis. Were I in the shoes of the DPC assessing that evidence, I would, at the very least, wish to interrogate TikTok about the third Xu opinion before accepting that it represented an adequate assessment of the legal position such that a suspension order was no longer appropriate or necessary. Of course, the opinion would have to be considered in light of the other information relied on by TikTok in relation to the suspension order, the Project Clover measures.

586. The position with the assessment of the pseudonymisation and privacy solutions is far more complex. It is clear from the Decision that the DPC did have regard to the evidence submitted. The Project Clover measures are described in detail, the Mittal Report is referenced, as are the Project Clover updates. It is also clear that the DPC considered, correctly, whether in light of that evidence, a suspension order was necessary, appropriate and proportionate. The DPC concluded that it was.

587. What is not at all clear is *why* it so concluded? It would appear from the fact that it carried out the assessment at all that the DPC considered that it was *possible* that the various privacy measures adopted by TikTok could have persuaded it that a suspension order was not required, though I accept that this may not be the case. If it was possible, then the DPC clearly was not persuaded, but the court and TikTok are at a loss to understand why. TikTok requested meetings with the DPC to discuss and explain its new measures, but no meeting

took place. Indeed, because of the time when this information was introduced by TikTok, post-PDD, there was no engagement between TikTok and the DPC on those measures at all, and nothing, accordingly, in the record which enables the court to understand how the DPC assessed them.

588. The question, in substance, for the court is whether the DPC *should* have been persuaded. However, to answer that question would require a deep understanding of enormously complex technical data, the subject of various expert reports submitted to the DPC, an expert body, in the Inquiry. The statutory scheme anticipates that it is the expert body which will first assess that information, not the court. Though the information was referred to during the course of the hearing, it was not interrogated in any detail, still less was it the subject of expert evidence for the purpose of explaining its significance.

589. On one view, I could determine that absent proving that the material *does* or *could* address the DPC's concerns, TikTok has failed to establish an error in the DPC's decision and that its appeal should, accordingly fail. However, where TikTok has not been informed of the reason that its material fell short, this would clearly be an unfair outcome. By the same token, a conclusion that because TikTok has identified an error in assessment, without establishing that the error may have been operative, it is nonetheless entitled to an order annulling the suspension order would plainly not be appropriate and would undermine the high level of protection of personal data demanded by the GDPR.

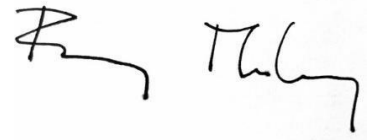
590. The statutory scheme envisages that the court should, accordingly, assess the evidence and determine the 'correct' outcome. However, the assessment of the evidence relevant to the pseudonymisation and privacy solutions employed by TikTok are matters which require considerable expertise. Although the courts can and do regularly assess expert evidence, this typically occurs with the help of expert witnesses to assist in explaining that evidence. Such assistance would be essential in understanding the evidence at issue in this case. I do not see how I could safely assess the evidence without it.

591. Moreover, the statutory scheme envisages that the court carry out the task of assessing technical evidence with the benefit of the DPC's prior assessment of that evidence, and its assessment of what if any a corrective order is appropriate, to which assessment the court is

required to afford deference. The statutory scheme would be frustrated if the court did not have the benefit of that assessment, and the reasons for the DPC's conclusions.

592. In the circumstances, it appears to me that in the very particular circumstances of this case, the appropriate order to make in substitution for the corrective orders is an order vacating the corrective orders and remitting the question of what corrective orders to make in light of the Article 46 infringement finding to the DPC for further consideration. Subject to hearing further from the parties on the final form of order, that is what I propose to do.

593. I will accordingly list these proceedings on 11 June 2026 at 10 am for the purpose of making final orders. I encourage the parties to engage with each other in advance of that date with a view to agreeing the form of order.

A handwritten signature in black ink, appearing to be 'R. M. L.', is located in the lower right quadrant of the page. The signature is written in a cursive, flowing style.