In the matter of the General Data Protection Regulation

DPC Case Reference: IN-21-9-2

In the matter of TikTok Technology Limited

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

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

Decision

Decision-Makers for the Data Protection Commission:

Dr Des Hogan, Commissioner for Data Protection and

Mr Dale Sunderland, Commissioner for Data Protection

30 April 2025

Data Protection Commission
6 Pembroke Row
Dublin, D02 X963
Ireland

Contents

A. Introduction

1. The General Data Protection Regulation[1] (the '**GDPR**') is a regulation in European Union law on the protection of individuals with regard to the processing of their personal data. The date of application of the GDPR is 25 May 2018. The Data Protection Commission (the '**DPC**') was established on 25 May 2018, pursuant to the Data Protection Act 2018 (the '**2018 Act**'), as Ireland's supervisory authority within the meaning of, and for the purposes specified in the GDPR.

2. This is a decision (the '**Decision**') of the DPC pursuant to section 111 of the 2018 Act and Article 60 of the GDPR. The DPC has made this Decision in the context of an own-volition inquiry bearing the reference number IN-21-9-2 ('**the Inquiry**') which was commenced on 14 September 2021 by the DPC under section 110 of the 2018 Act in respect of TikTok Technology Limited ('**TikTok Ireland**').

3. This Decision sets out the DPC's findings in this matter as to whether (i) an infringement of a relevant enactment by TikTok Ireland, the controller to which the Inquiry relates, has occurred or is occurring, (ii) if so, whether a corrective power should be exercised in respect of TikTok Ireland as the controller concerned, and the corrective power that is to be so exercised. An infringement of a relevant enactment, for this purpose, means an infringement of the GDPR, or an infringement of a provision of, or regulation under, the 2018 Act which gives further effect to the GDPR.[2]

4. A preliminary draft of this document (the '**Preliminary Draft Decision**') was provided to TikTok Ireland for the purpose of allowing it to make submissions as to the provisional findings outlined in that Preliminary Draft Decision. TikTok Ireland made submissions in response to the Preliminary Draft Decision. In preparing this Decision, the DPC has taken into account the submissions and observations made in response to the Inquiry, as well as other relevant information as set out in this Decision. The Preliminary Draft Decision was revised to take account of TikTok Ireland's submissions before submitting a draft version of this Decision (the '**Draft Decision**') to the process prescribed by Article 60 GDPR.

5. On 21 February 2025, the DPC submitted that Draft Decision to concerned supervisory authorities for their views, in accordance with Article 4(22) and Article 60(3) GDPR. Given that the cross-border processing under examination entailed the processing of personal data throughout Europe, all other EU/EEA data protection supervisory authorities (the '**SAs**', each one being an '**SA**') were engaged as a concerned supervisory authority ('**CSA**') for the purpose of the cooperation process outlined in Article 60 GDPR. The CSAs expressed their views in response to the Draft Decision as follows:

    (i) The Netherlands SA exchanged a comment on 20 March 2025;

    (ii) The French SA exchanged a comment on 21 March 2025; and

    (iii) The German SAs (via the Berlin DPA) exchanged a comment on 21 March 2025.

    collectively referred to as ('**CSA Comments**').

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Sections 105(1) and 107 of the 2018 Act.

6. No concerned supervisory authority submitted an objection to the Draft Decision.

7. In overview, this Inquiry is concerned with an examination of TikTok Ireland's compliance with the requirements of the GDPR as they relate to the transfer of personal data of users of the TikTok platform in the EEA[3] ('**EEA User Data**') to a third country,[4] the People's Republic of China ('**China**'), under Chapter V GDPR, and the provision of information to users in relation to such transfers as required by Article 13(1)(f) GDPR.

8. The GDPR provides a high level of protection of personal data throughout the EEA and provides data protection rights to individuals. When personal data is transferred outside of the EEA this can impede the ability of natural persons to exercise data protection rights and can circumvent that high level of protection. Therefore, it is crucial that the level of protection ensured by the GDPR should not be undermined in the case of such transfers. Accordingly, transfers of personal data can take place only if the conditions laid down in Chapter V of the GDPR are complied with. This ensures that the high level of protection provided within the European Union continues where personal data is transferred to a third country.

B. Preliminary Matters

a) Controller

9. TikTok Technology Limited (referred to throughout this Decision as '**TikTok Ireland**') is a private company limited by shares registered in Ireland under company number 635755 and having its registered office at The Sorting Office, Ropemaker Place, Dublin 2, Dublin, D02 HD23, Ireland. TikTok Ireland is part of the ByteDance group of multinational technology companies.

10. TikTok Ireland has confirmed that TikTok Ireland and TikTok Information Technologies UK Limited ('**TikTok UK**') are joint controllers of personal data of users of the TikTok platform and associated services in the European Economic Area, Switzerland and the United Kingdom. In particular, TikTok Ireland provides the TikTok platform to users in the EEA ('**EEA users**') and users in Switzerland, and TikTok UK provides the TikTok platform to users in the United Kingdom.[5] The DPC is satisfied in light of the information obtained in the Inquiry that TikTok Ireland is the controller within the meaning of Article 4(7) GDPR in respect of the processing of personal data of users of the TikTok platform in the EEA.

11. The scope of this Inquiry is directed solely to TikTok Ireland in respect of the processing of personal data of EEA users of the TikTok platform. It is not directed to processing of personal data of users of the TikTok platform in Switzerland or the United Kingdom.

b) Competence of the DPC as lead supervisory authority

12. Chapter VI, Section 2, of the GDPR deals with the competence, tasks and powers of the supervisory authorities. Article 55(1) GDPR provides that each supervisory authority shall be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it in accordance with the GDPR on the territory of its own Member State. Article 56(1) GDPR states:

---

[3] "The EEA" means the European Economic Area and includes the Member States of the European Union, and Iceland, Norway and Liechtenstein.
[4] "Third country" means any country that is not part of the EEA.
[5] TikTok Ireland's Response dated 12 October 2021, at page 1, and TikTok Ireland's Response dated 20 June 2022, at page 1.

> 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.

13. The concept of the "*main establishment*" of a controller is defined in Article 4(16)(a) GDPR to mean:

> as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

14. The concept of *"cross-border processing*" is further defined in Article 4(23) GDPR as follows:

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

15. As outlined above, TikTok Ireland has confirmed in the Inquiry that TikTok Ireland provides the TikTok platform to users in the EEA.

16. It is relevant in this regard to note that in the context of engagement by the DPC with TikTok Ireland in 2020, the DPC assessed and was ultimately satisfied that as of 29 July 2020, (i) TikTok Ireland was in a position to demonstrate effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements, and (ii) as between TikTok Ireland, TikTok UK and the other TikTok affiliates in the EU, only TikTok Ireland could make the final determination in relation to data processing matters that related to EEA users and only TikTok Ireland could have such decisions implemented. The DPC was therefore satisfied that that TikTok Ireland had its main establishment within the meaning of Article 4(16) GDPR in Ireland[6].

17. It is also clear that in providing the TikTok platform to users in the EEA, TikTok Ireland engages in cross-border processing within the meaning of Article 4(23) GDPR.

18. Having regard to the above, the DPC is satisfied that TikTok Ireland:

> (i) acts as the controller within the meaning of Article 4(7) GDPR in respect of the processing of personal data of users of the TikTok platform in the EEA,
>
> (ii) has its main establishment within the meaning of Article 4(16) GDPR in Ireland, and
>
> (iii) engages in cross-border processing of personal data within the meaning of Article 4(23) GDPR.

[6] Letter from the DPC to TikTok Ireland dated 22 December 2020.

19. The DPC is satisfied that the above was the position at all material times since 29 July 2020.

20. Accordingly, the DPC is satisfied that the DPC is competent to act as lead supervisory authority within the meaning of Article 56(1) GDPR of TikTok Ireland for the cross-border processing of personal data of EEA users carried out by TikTok Ireland that is the subject of this Inquiry in accordance with the procedure provided for in Article 60 GDPR.

c) Functions and powers of the DPC relevant to the Inquiry

The Charter of Fundamental Rights of the European Union

21. The GDPR elaborates on the indivisible, universal values of human dignity, freedom, equality and solidarity as enshrined in the Charter of Fundamental Rights of the EU ('**the Charter**') and Article 8 in particular, which safeguards the protection of personal data. Article 8 of the Charter provides:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2.Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

The GDPR

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

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

24. Article 56(1) GDPR provides that, without prejudice to GDPR 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 GDPR.

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

> "monitor and enforce the application" of the GDPR (Article 57(1)(a) GDPR),
>
> "cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of" of the GDPR (Article 57(1)(g) GDPR),
>
> "conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority" (Article 57(1)(h) GDPR),

> "monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices" (Article 57(1)(i) GDPR), and
>
> "fulfil any other tasks related to the protection of personal data" (Article 57(1)(v) GDPR).

26. Interpreting Articles 55(1) and 57(1)(a) GDPR in the judgment of the Court of Justice of the European Union ('**the CJEU**'), delivered on 16 July 2020, in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems[7] ('**the Schrems II judgment**') the CJEU noted that:

> In accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data. Each of those authorities is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in that regulation.[8]

27. The CJEU further observed that:

> It follows from those provisions that the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement. The exercise of that responsibility is of particular importance where personal data is transferred to a third country since, as is clear from recital 116 of that regulation, 'when personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information'. In such cases, as is stated in that recital, 'supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders'.[9]

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

> (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
>
> (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
>
> (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
>
> (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

---

[7] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559).
[8] At paragraph 107.
[9] At paragraph 108.

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

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

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

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

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

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

29. It is further relevant to note for present purposes that:

(i) Article 60 GDPR provides for a system of cooperation between the lead supervisory authority and the other supervisory authorities concerned,

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

(iii) Article 65 provides that the European Data Protection Board (the **''EDPB''**) may engage in dispute resolution, inter alia, in cases to which Article 60(4) GDPR applies.

The Data Protection Act 2018

30. The powers of the DPC in the context of the Inquiry are further regulated by sections 110, 111 and 115 of the 2018 Act.

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

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

(1) Where an inquiry has been conducted of the Commission's own volition, the Commission, having considered the information obtained in the inquiry, shall –

(a) If satisfied that an infringement by the controller or process to which the Inquiry relates has occurred or is occurring, make a decision to that effect, and

(b) If not so satisfied, make a decision to that effect.

(2) Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision –

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

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

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

33. The application of Sections 110 and 111 in the context of the present inquiry is subject to Article 60 of the GDPR, in circumstances where the processing the subject of the Inquiry constitutes cross-border processing within the meaning of that term as defined at Article 4(23) GDPR.

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

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

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

35. Section 107 defines the term "*corrective power*" for the purpose of these provisions as "*a power conferred by Article 58(2)"* of the GDPR, set out above.

C. Context for the Inquiry and materials considered for the purposes of the Inquiry

a) The TikTok platform

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.[10]

37. The TikTok platform is understood to have more than 1 billion monthly active users globally as of 27 September 2021.[11] TikTok Ireland has informed the DPC that in May 2022, the TikTok platform had approximately [redacted] users in the EEA.[12] 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.[13]

[10] Direct messaging on TikTok is only available to registered account holders aged 16 and older.
[11] See <https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok>.
[12] TikTok Ireland's Response dated 20 June 2022, at page 4.
[13] https://www.tiktok.com/transparency/en/eu-mau-2024-12.

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. It has stated that personal data of EEA users is segregated and stored separately from personal data of users of Douyin.[14]

39. In response to a query by the DPC, TikTok Ireland has advised that TikTok does not share EEA User Data with other ByteDance companies in China for use in other ByteDance products (including Toutiao and Douyin).[15]

b) Background to the Inquiry

40. The background to the Inquiry is set out in the Commencement Notice dated 14 September 2021 at paragraphs 1–5. In brief overview:

(i) On 28 May and 5 July 2021 respectively, the French Supervisory Authority - Commission Nationale de l'Informatique et des Libertés ('**CNIL**') requested the DPC to provide mutual assistance in accordance with Article 61 GDPR by commencing a statutory inquiry in respect of the subject matter of the CNIL's investigation commenced prior to 29 July 2020. The CNIL investigation concerned the processing of personal data (including that of child users) based on an online examination of the TikTok app and website tiktok.com. The CNIL requested that the DPC investigate matters pertaining to TikTok's transfers of personal data.

(ii) On 7 April 2021, the DPC received by letter a submission from Stichting Onderzoek Marktinformatie ('**the SOMI Submission**') raising concerns about the processing of personal data by TikTok. SOMI requested that the DPC investigate activities of TikTok (which SOMI claimed give rise to infringements of the GDPR), due to risks for young users and risks concerning the non-EEA transfers of personal data.

(iii) During the course of its supervision interactions with TikTok Ireland, the DPC was informed by TikTok Ireland that certain personnel located in China access EEA personal data of TikTok users in order to provide support services in connection with the operation of the Platform, including functions related to software engineering, maintenance and development.

41. On 26 March 2021, upon request of the DPC, TikTok Ireland provided the DPC with its Data Transfer Assessment for China along with other supporting documentation ('**the March 2021 Data Transfer Assessment**').

42. Against that background, on 14 September 2021, the DPC notified TikTok Ireland of the commencement of two inquiries under Section 110 of the 2018 Act, namely (i) this Inquiry, and (ii) a further separate Inquiry relating to the processing of personal data of child users of the TikTok platform ("**the Child Users' Data Inquiry**').

---

[14] TikTok Ireland's Response dated 12 October 2021, at pages 1 and 2, and Response dated 20 June 2022, at page 3.

[15] TikTok Ireland's Response dated 20 June 2022, at page 8.

43. While initially it was envisaged that the inquiries would be conducted concurrently[16], ultimately the inquiries were conducted and progressed separately. A final decision in the Child Users' Data Inquiry was adopted on 1 September 2023. The DPC outlined at paragraph 29 of the Commencement Notice dated 14 September 2022, and later by letter to TikTok Ireland dated 3 October 2022, that if the DPC at any time formed the view that it was necessary to rely on or have regard to information or documentation obtained in the Child Users' Data Inquiry for the purposes of this present Inquiry, the DPC would notify TikTok Ireland in writing, and, if such documentation or information was not obtained directly from TikTok Ireland, provide TikTok Ireland with a copy of same.[17] The DPC confirms that, in the event, no information or documentation obtained in the Child User's Data Inquiry was used or considered for the purpose of this Inquiry.

c) Conduct of the Inquiry

44. The following is a summary of the main stages in the Inquiry.

i. Commencement of the Inquiry

45. As set out previously above, the Inquiry was initiated by Commencement Notice dated 14 September 2021. TikTok Ireland was requested to respond in a comprehensive manner to each of the queries set out at Appendix 1 to the notice by 12 October 2021. TikTok Ireland duly provided its response within that timeframe, with a schedule of supporting documents ('**TikTok's Response dated 12 October 2021**'). This response included including TikTok Ireland's October 2021 Data Transfer Assessment ('**the October 2021 Data Transfer Assessment**'). The DPC responded to confidentiality concerns articulated in TikTok Ireland's response.

46. On 20 January 2022, TikTok Ireland notified the DPC that it had recently performed an update to its Data Transfer Assessments for certain third countries. On 28 January, TikTok Ireland provided the DPC with those updated Data Transfer Assessments, and confirmed that the Data Transfer Assessment for China was the same as that submitted as part of TikTok Ireland's response dated 12 October 2021. On 1 February 2022, the DPC responded to that correspondence.

ii. Request for Further Information

47. By letter dated 11 May 2022, the DPC requested further information arising from the information and documents provided by TikTok Ireland in the Inquiry, with an initial date for response by 1 June 2022. By letter dated 16 May 2022, TikTok Ireland requested additional time to respond to the queries, seeking an extension of time to 6 July 2022. By letter dated 17 May 2022, the DPC allowed an extension of time to 15 June 2022. TikTok Ireland furnished its responses, with a schedule of supporting documents on 17 June 2022 ("**TikTok Ireland's Response dated 17 June 2022**'). On 20 June 2022, TikTok Ireland sent an amended version of its initial response ('**TikTok Ireland's Response dated 20 June 2022**').

[16] Commencement Notice dated 14 September 2021, paragraph 29.
[17] Commencement Notice dated 14 September 2021, paragraph 29 and letter from the DPC to TikTok Ireland dated 3 October 2022.

iii. Statement of Issues

48. The DPC furnished TikTok Ireland with a Statement of Issues in the Inquiry on 7 July 2022 ('**the Statement of Issues**'). The purpose of the Statement of Issues was (i) to identify the issues which, in the DPC's view, would require to be considered and determined in the Inquiry in a draft decision by the DPC for the purpose of section 111 of the 2018 Act and Article 60 GDPR, and (ii) to enable TikTok Ireland to make any further submissions or comments it wished to make as to the issues so identified. The DPC requested that TikTok Ireland provide a response to the Statement of Issues by 4 August 2022.

49. In the Statement of Issues, the DPC had indicated its intention to consider the information set out in Section 2.1 of the *"Final Report EDPS/2019/02-13, Legal study on Government access to data in third countries for the EDPB (November 2021)"* ('**Milieu Report**').[18]

50. By letter dated 12 July 2022, TikTok Ireland made a reasoned request for an extension of time to provide its response to the Statement of Issues by six weeks to 15 September 2022. Having duly considered TikTok Ireland's request, by letter dated 12 July 2022, the DPC extended the deadline to 15 September 2022.

51. By letter dated 19 July 2022, TikTok Ireland raised certain queries with the DPC relating to the factual summary outlined in the Statement of Issues. The DPC made a reply to those queries by further letter dated 25 July 2022.

iv. Submission on the Statement of Issues

52. TikTok Ireland furnished its submission on the Statement of Issues on 15 September 2022 ('**TikTok Ireland's Submission dated 15 September 2022**').

53. By its letter dated 15 September 2022 enclosing the Statement of Issues, TikTok Ireland informed the DPC of its intention to submit expert evidence in the Inquiry. TikTok Ireland informed the DPC that it intended to submit expert evidence from an independent expert based in China in order to make submissions in respect of the content of the Milieu Report, and requested a further period of four weeks within which to do so, by 13 October 2022.

54. TikTok Ireland further informed the DPC that:

    (i) it was in the process of updating its Data Transfer Assessment for China and expected to complete the update within a period of four weeks, that is, by 13 October 2022,

    (ii) it was also in the process of updating its EEA Privacy Policy, and would provide the DPC with the relevant part of the updated Privacy Policy prior to it being published online and notified to users.

55. Further, TikTok Ireland advised in its letter dated 15 September 2022 that TikTok Ireland would shortly be amending and replacing its Intra-Group Agreement for the purposes of transitioning from the SCCs contained in the annex to the European Commission Decision 2010/87/EU of 5 October 2010 ('**the 2010 SCCs**') to module two (controller to processor) of the standard contractual clauses for the transfer of personal data to

[18] Final Report EDPS/2019/02-13, Legal study on Government access to data in third countries for the EDPB (November 2021), <https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en>.

processors established in third countries pursuant to Regulation (EU) 2016/679 adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2022 ('**the 2021 SCCs**').

56. TikTok Ireland indicated that it was in the process of updating the Intra-Group Agreement before the deadline of 27 December 2022 and would provide the DPC with a copy of the updated contractual agreement in due course.

57. On 13 October 2022, TikTok Ireland provided an expert opinion of Professor Ke Xu ('**the First Xu Report**')[19], Associate Professor of the Law School of the University of International Economics in Beijing ('**UIBE**') and Director of the Digital Economy and Legal Innovation Research Centre of UIBE. The scope of this opinion was to *"to consider whether the Milieu Report, with respect to Chinese law and practice, is inaccurate in any respects and to provide any other observations with respect to the Milieu Report which may be relevant to the Inquiry"*.[20]

v. Data Transfer Assessment Submissions

58. In addition to the October 2021 Data Transfer Assessment, TikTok Ireland submitted a number of additional updated Data Transfer Assessments during the course of the Inquiry.

59. On 13 October 2022, TikTok Ireland submitted an updated Data Transfer Assessment for transfers to China under the 2010 SCCs.

60. On 19 December 2022, TikTok Ireland submitted a Data Transfer Assessment for transfers to China under the 2021 SCCs.

61. On 6 October 2023, TikTok Ireland submitted an updated Data Transfer Assessment for transfers to China under the 2021 SCCs.

62. On 31 July 2024, TikTok Ireland submitted an updated Data Transfer Assessment for transfers to China under the 2021 SCCs.

vi. Updated EEA Privacy Policy

63. By letters dated 22 and 26 October 2022, TikTok Ireland informed the DPC that the intended update to its EEA Privacy Policy would be notified to users on 28 October 2022 and would take effect from 27 November 2022, and requested that the update be taken into account by the DPC for the purpose of the Inquiry. A copy of the updated parts of the Privacy Policy that were relevant to the Inquiry was provided with those letters.

64. On 3 November 2022, TikTok Ireland confirmed that the Privacy Policy was launched from 2 November 2022 and would be effective from 2 December 2022.

---

[19] The First Xu Report describes that Professor Ke Xu holds a PHD in law under the joint training of UIBE and University of California, Berkeley. Professor Ke Xu is one of two initiators of the China Personal Information Protection and Data Governance Thirty Person Forum, a member of the World Data Governance and Cyber Security Research Alliance Secretariat, and a director of the China Cyber Information Law Institute. The report sets out that Professor Ke Xu has 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. Professor Ke Xu, as a co-author, has also published On Cyber Sovereignty (Social Science Academic Press, 2017), Big Data, AI and People (Peking University Press, 2019) and other books.

[20] The First Xu Report, at page 1.

65. On 3 April 2023, TikTok Ireland notified the DPC of another change to its Privacy Policy, to accommodate, inter alia, data storage in a Malaysian data centre.

vii. Submission relating to the 2021 SCCs

66. By letter dated 3 October 2022, the DPC confirmed, in response to a query raised in TikTok Ireland's Response to the Statement of Issues, that the temporal scope of the Inquiry was concerned with transfers (as defined in the context of the Inquiry) taking place from 29 July 2020.

67. The DPC noted, however, that:

(i) TikTok Ireland was in the process of transitioning to the 2021 SCCs in advance of the deadline of 27 December 2022, and

(ii) in that context, TikTok Ireland intended to submit to the DPC a copy of the updated Intra-Group Agreement implementing the 2021 SCCs, and of the updated Data Transfer Assessment in the context of the Inquiry.

68. Where it had become apparent that TikTok Ireland would be transitioning to the 2021 SCCs while the present Inquiry is in progress, and prior to the issuing of a preliminary draft decision, the DPC proposed in its letter dated 3 October 2022 that information, documentation, or submissions relating to the updated position under the 2021 SCCs that TikTok Ireland provided in advance of the issuing of the Preliminary Draft Decision in the Inquiry would be considered and taken into account by the DPC for the purpose of the Preliminary Draft Decision, and that TikTok Ireland would then be invited to make further submissions as to the updated position under the 2021 SCCs together with its submissions in response to the Preliminary Draft Decision. TikTok Ireland was invited to express its view on that proposed approach by 24 October 2022.

69. By letter dated 23 October 2022, TikTok Ireland confirmed that it wished to make submissions in respect of the updated position arising from its transition to the 2021 SCCs prior to the issue of the Preliminary Draft Decision in the Inquiry. It stated that it was necessary to satisfy the requirements of fair procedures that the DPC receive and consider its submissions on the 2021 SCCs in advance of preparing the preliminary draft decision.

70. By letter dated 1 November 2022, the DPC noted the position as set out in TikTok Ireland's letter dated 23 October 2022, and agreed to receive TikTok Ireland's updated Intra-Group Agreement implementing the 2021 SCCs and updated Data Transfer Assessment for China, together with any submissions TikTok Ireland wished to make in respect of same by no later than 9 December 2022.

71. By letter dated 8 December 2022, TikTok Ireland wrote to the DPC seeking an extension of time within which to furnish its updated Intra-Group Agreement and submissions to 19 December 2022. The DPC duly acceded to this request by letter dated 9 December 2022.

72. TikTok Ireland provided the relevant submissions and documentation relating to the 2021 SCCs on 19 December 2022 ('**TikTok Ireland's Submission dated 19 December 2022**').

73. By letter dated 21 February 2023, the DPC sent a request for further information in respect of matters arising from TikTok Ireland's Submission dated 19 December 2022 and seeking a response by 14 March 2023. TikTok Ireland requested an extension to that deadline by letter dated 22 February 2023, and by reply of the same date the DPC granted the requested extension to 28 March 2023. TikTok Ireland's reply was duly received by the DPC on 28 March 2023.

74. By its letter dated 21 February 2023, the DPC also confirmed to TikTok Ireland, further to a point raised in TikTok Ireland's Submission dated 19 December 2022, that the DPC did not propose to make changes to the Issues for Determination in the Inquiry, save to the extent that, where the Issues for Determination referred

to the 2010 SCCs, this should now be taken to refer additionally to the 2021 SCCs. This arose in a context where TikTok Ireland was afforded the opportunity to address any changes to the analysis due to the 2021 SCCs, in circumstances where TikTok Ireland had transitioned to the 2021 SCCs while the Inquiry remained in progress, and prior to the issuing of a preliminary draft decision in the Inquiry.

75. On 26 April 2023, the DPC wrote to TikTok Ireland setting out the concept of undertaking and how it applies in the context of the GDPR and detailing the DPC's understanding of the relevant factors, as they appeared to apply to TikTok Ireland. TikTok Ireland responded to that letter on 12 May 2023 the DPC has had regard to those responses where relevant as set out below.

76. On 2 May 2023, TikTok Ireland raised queries with the DPC regarding reports in the media regarding comments made by a spokesman of the Department of Communications in Ireland. The DPC responded to these queries on 8 May 2023.

viii. Preliminary Draft Decision

77. On 17 May 2023, the DPC wrote to TikTok Ireland and provided it with its Preliminary Draft Decision on the Inquiry. The Preliminary Draft Decision set out the DPC's provisional findings and invited submissions from TikTok Ireland on any matters of fact or law which pertain to the provisional findings contained therein.

78. On 9 September 2023, TikTok Ireland made both factual and legal submissions in response to the Preliminary Draft Decision. The DPC has had regard to those submissions in preparing this Decision.

79. TikTok Ireland's submissions in response to the Preliminary Draft Decision also included what it described as a *"Supplemental expert report"*, dated 8 September 2023, of Professor Ke Xu ('**the Second Xu Report**'). The title to this report is *"Related Chinese law issues in response to the Irish Data Protection Commission's ("DPC") Inquiry IN-21-9-2 (the "Inquiry") into TikTok Technology Limited ("TikTok")"*. The submissions also included a technical report setting out project milestones and timelines for the completion of Project Clover (the '**Project Clover Technical Report**'). TikTok Ireland has described Project Clover as *"a program focused on creating a secure enclave for EEA User Data with sophisticated controls governing access"*[21]. The Project Clover Technical Report outlined that [redacted]

80. On 29 September 2023, TikTok Ireland provided the DPC with its updated European Transfer Matrix that sets out the China Group Entities that have remote access to EEA User Data, reflecting changes in the China Group Entities. TikTok Ireland also provided the DPC with an expert report prepared by Professor Prateek Mittal[22] (the '**Mittal Report**') regarding differential privacy measures to be taken as part of Project Clover.

81. On 6 October 2023, TikTok Ireland provided the DPC with an updated Data Transfer Assessment, which it stated was to account for:

[21] TikTok Ireland's responses dated 28 March 2023.

[22] The Mittal Report sets out that Professor Mittal is a Professor in the Department of Electrical and Computer Engineering at Princeton University, and is 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. Professor Mittal received graduate degrees in Electrical and Computer Engineering from the University of Illinois at Urbana-Champaign (M.S in 2010, Ph.D. in 2012). Professor Mittal has published over 100 papers at peer-reviewed conferences and journals in the field of privacy and security.

(i) Certain developments in Chinese law and practice;

(ii) Additional information that has come to TikTok Ireland's attention;

(iii) Changes to the China Group Entities;

(iv) Changes in supplementary measures in place, including as a result of implementation of [redacted] Project Clover; and

(v) Updates to the structure of the Data Transfer Assessment.

82. On 8 February 2024, the DPC wrote to TikTok Ireland with queries seeking clarification on matters regarding TikTok Ireland's response to the Preliminary Draft Decision and requiring TikTok Ireland to respond by 22 February 2024. TikTok Ireland requested an extension to that deadline and the DPC granted an extension until 7 March 2024.

83. On 22 February 2024, TikTok Ireland wrote to the DPC requesting the DPC to confirm the contact details of the Commissioner to whom future correspondence in this Inquiry should be addressed. On 4 March 2024, the DPC confirmed that future correspondence should be addressed to the Commission and marked for the attention of Commissioners Hogan and Sunderland, the Decision-Makers for the DPC in this Inquiry.[23]

84. On 6 March 2024, TikTok Ireland wrote to the DPC informing it that TikTok Ireland would not be able to respond to the queries set out in the DPC's letter of 8 February 2024 by 7 March 2024. On 11 March 2024, TikTok Ireland responded to those queries.

85. On 26 March 2024, TikTok Ireland wrote to the DPC referring to the supplementary measures that it has implemented since the Preliminary Draft Decision. TikTok Ireland stated that since it provided its response to the Preliminary Draft Decision on 8 September 2023, progress on implementing Project Clover had continued at pace, [redacted]

86. On 15 April 2024, the DPC confirmed to TikTok Ireland that it would consider all information submitted by TikTok Ireland in the Inquiry when making its Draft Decision, including all information submitted by TikTok Ireland in respect of Project Clover. The DPC also informed TikTok Ireland that any additional information that it has not yet provided to the Inquiry should be provided in writing.

87. On 18 April 2024, TikTok Ireland confirmed that it would provide further information on Project Clover in writing. On 26 April 2024, TikTok Ireland confirmed that it would provide that information by 17 May 2024. On 29 April 2024, TikTok Ireland made submissions regarding the confidentiality of information previously submitted.

88. On 17 May 2024, TikTok Ireland wrote to the DPC providing a detailed update about the new measures implemented as part of Project Clover, including in respect of changes made since TikTok Ireland's submission in response to the Preliminary Draft Decision on 9 September 2023. TikTok Ireland also sought a Revised Preliminary Draft Decision from the DPC to reflect additional safeguards and new security measures that it stated had been implemented under Project Clover. On 14 June 2024, TikTok Ireland wrote to the DPC reiterating its position that the DPC should issue a Revised Preliminary Draft Decision.

89. On 21 June 2024, the DPC wrote to TikTok Ireland setting out its position that it did not consider that it would be necessary to prepare a Revised Preliminary Draft Decision and that the DPC would continue to progress

[23] On 20 February 2024 Commissioners Hogan and Sunderland were appointed as Commissioners for Data Protection by the Minister for Justice pursuant to an independent appointments process.

its Draft Decision for the purposes of Article 60(3) GDPR. The DPC also requested TikTok Ireland to confirm the 2023 turnover of ByteDance Ltd.

90. On 28 June 2024, TikTok Ireland wrote to the DPC reiterating its view that the DPC ought to issue a Revised Preliminary Draft Decision. TikTok Ireland also confirmed the 2023 turnover of ByteDance Ltd, while setting out its view that this turnover is not a relevant consideration in setting any administrative fine. TikTok Ireland also informed the DPC that it was in the process of updating its Data Transfer Assessment and that the update would be complete by the end of July.

91. On 31 July 2024, TikTok Ireland provided the DPC with its updated Data Transfer Assessment. This updated Data Transfer Assessment reflected how the additional protections outlined in the submissions of 17 May 2024 had been largely implemented at that point.

92. On 2 October 2024, TikTok Ireland provided the DPC with the audited consolidated turnover for TikTok UK, including that of TikTok Ireland, for the financial year ending 31 December 2023. TikTok Ireland reiterated its position that a Revised Preliminary Draft Decision was required.

93. On 6 December 2024, TikTok Ireland provided the DPC with its updated European Transfer Matrix and Intra Group Transfer Agreement reflecting updates made as a result of Project Clover. These changes were made to the European Transfer Matrix and the 2022 Intra Group Agreement was otherwise unchanged.

94. On 14 February 2025, TikTok Ireland informed the DPC that it was preparing a further update on Project Clover and that it was aiming to share that update with the DPC by 10 March 2025.

ix. The Draft Decision

95. On 21 February 2025, the DPC prepared and circulated the Draft Decision to the CSAs. On the same date, the DPC also provided TikTok Ireland with a copy of the Draft Decision. Given that the matters under examination in the Inquiry entail cross-border processing across Europe, all other supervisory authorities were engaged as CSAs for the purpose of the co-decision-making process outlined in Article 60 GDPR. No objections to the Draft Decision were raised during the prescribed four-week consultation period. Comments were exchanged by the supervisory authorities of France, the Netherlands, and Berlin. The DPC has taken account of those views expressed in those comments in preparing this Decision.

96. On 14 March 2025, TikTok Ireland requested the DPC to withdraw the Draft Decision from the Article 60 process. On 18 March 2025, TikTok Ireland provided the DPC with an Expert Opinion, dated 18 March 2025, of Professor Ke Xu ('**the Third Xu Report**'). The title to this report is *"Related Chinese law issues in response to the Irish Data Protection Commission's ("DPC") Inquiry IN-21-9-2 (the "Inquiry") into TikTok Technology Limited ("TikTok")"*.

97. On 21 March 2025, TikTok Ireland informed the DPC that *"certain developments and matters that have come to our attention which will require the correction and/or clarification of statements previously made by TikTok Technology Limited to the DPC concerning the circumstances in which transfers of EEA User Data are made and the manner in which Clover operates."* TikTok Ireland informed the DPC that it was in the process of putting together a complete update.

98. On 25 March 2025, the DPC wrote to TikTok Ireland informing it that it would not be withdrawing the Draft Decision from the Article 60 process and rejecting the basis put forward by TikTok Ireland for its request. The DPC also informed TikTok Ireland that the DPC received a total of three comments from the CSAs in respect of the Draft Decision. The DPC provided those comments to TikTok Ireland on 25 March 2025 when the DPC provided TikTok Ireland with proposed limited non-material amendments to the Draft Decision that the DPC proposed to make further to its obligation to take due account of the views expressed by the CSAs. The DPC

invited submissions from TikTok Ireland on (1) these proposed amendments and (2) on the assessments and material that would form the basis for the DPC's final determination of the quantum of the administrative fines to be imposed in the Final Decision. A two week period for submissions was given. As set out below, TikTok Ireland made submissions on 11 April 2025. The DPC has given full regard to these submissions in preparing this Decision, including TikTok Ireland's assertion that the DPC ought not to make certain proposed changes, arguing that three proposed changes are material in nature. The DPC has reflected on this submission and has satisfied itself that the changes that the DPC has now implemented below are not material in nature. They are not material in nature in circumstances where they do not reflect substantial changes to any aspect of the Draft Decision. In particular, the amendments do not add to, or detract from, the Draft Decision in any material way, nor do they operate to disturb or alter, in any way, the positions and proposed findings that were reflected in the Draft Decision.

99. On 27 March 2025, TikTok Ireland sought certain information and clarifications regarding the finalisation of the Draft Decision. On 28 March 2025, TikTok Ireland sought an extension to the deadline for it to furnish the DPC with any submissions prior to the adoption of the final decision. TikTok Ireland also stated that ByteDance Ltd.'s audited accounts for the financial year ending 31 December 2024 were due to be finalised in the third week of April and accordingly sought an extension for the provision of that information until 18 April 2025.

100. On 2 April 2025, the DPC responded to TikTok Ireland's requests of 27 March 2025 and acceded to TikTok Ireland's request for an extension on the deadline for submissions.

101. On 9 April 2025, TikTok Ireland wrote to the DPC referring to reports in the media regarding the Inquiry and inquiring as to whether the DPC or other supervisory authorities have any knowledge of the source of disclosure of information relating to the inquiry which appeared in the media.

102. On 11 April 2025, TikTok Ireland provided the DPC with two letters. The first letter provided the DPC with TikTok Ireland's submissions on the proposed amendments to the Draft Decision and on the quantum of the fine. The second letter outlined inaccurate statements previously made by TikTok Ireland to the Inquiry in relation to the circumstances in which transfers of EEA User Data are made and the manner in which Project Clover operates. These inaccuracies are detailed further below regarding the material scope of this Decision. In the second letter, TikTok Ireland also provided the DPC with an update on Project Clover.

103. On 16 April 2025, the DPC responded to TikTok Ireland's letter dated 9 April 2025. The DPC also posed a number of queries to TikTok Ireland regarding the inaccurate information that TikTok Ireland submitted to the Inquiry. The DPC informed TikTok Ireland that it was required to urgently reply to those queries. On 16 April 2025, TikTok Ireland wrote to the DPC stating that, contrary to the position set out in its letter of 28 March 2025, the audited turnover figures for ByteDance Ltd were now expected either in the week of 5 May 2025 or no later than 15 May 2025. TikTok Ireland stated that it was willing to provide unaudited turnover figures for the purposes of the Final Decision.

104. On 17 April 2025, the DPC wrote to TikTok Ireland agreeing to TikTok Ireland's proposal to provide the unaudited turnover figures.

105. On 21 April 2025, TikTok Ireland provided the DPC with the unaudited annual turnover figure for ByteDance Ltd for the year ending 31 December 2024.

106. On 24 April 2025, TikTok Ireland responded to the DPC's queries regarding the inaccurate information that TikTok Ireland submitted to the Inquiry.

x. Fair procedures

107. Having reviewed the correspondence in the Inquiry (including those representations made by TikTok Ireland specifically directed to the fairness of the procedures adopted by the DPC and the DPC's replies to same) and recalling the extensive opportunities afforded to TikTok Ireland over a number of years to provide additional submissions and additional information to the Inquiry, including responses to DPC questions, submissions on the Inquiry Statement of Issues, submissions on the Preliminary Draft Decision, and further submissions following those submissions, the DPC is satisfied that the Inquiry was correctly conducted and that fair procedures were afforded to TikTok Ireland by the DPC. This includes, but is not limited to, the steps taken by the DPC to: (i) notify TikTok Ireland of the issues under examination in the Inquiry and the information and documentation required by the DPC, (ii) provide TikTok Ireland with an opportunity to provide updated responses and submissions in respect of the issues under consideration in the Inquiry at appropriate stages, (iii) provide TikTok Ireland with sufficient time to furnish the information and documentation requested by the DPC during the course of the Inquiry and (iv) to make submissions on a number of changes the DPC proposed to make to the Draft Decision to take account of the CSA views. The DPC has also carefully taken due note and account of all submissions and information submitted by TikTok Ireland in the past 4 years.

D. Issues and Scope

a) Scope

108. The Inquiry is concerned with the transfer of EEA User Data to China under the 2010 SCCs and the 2021 SCCs. Throughout the Inquiry, TikTok Ireland informed the DPC that those transfers of EEA User Data occurred by means of remote access only, whereby personnel in China remotely access EEA User Data in circumstances where that data is stored on servers located outside of China ('**the Remote Access Solution**'). TikTok Ireland consistently maintained throughout the Inquiry that the personal data of EEA users of TikTok was not stored on servers in China. This Decision, being the conclusion of a cross-border inquiry under Article 60 GDPR, is based on the assertions and representations of TikTok Ireland throughout the Inquiry that no EEA data is stored on servers in China.

109. On 9 April 2025, TikTok Ireland wrote to the DPC *"to provide details of developments and matters that have come to our attention which require the correction or clarification of statements previously made by TikTok Technology Limited ("TikTok Ireland") to the DPC in relation to the circumstances in which transfers of EEA User Data are made and the manner in which Clover operates."*

110. In that correspondence, TikTok Ireland stated that, on 19 February 2025, it was informed of an issue that resulted in some EEA User Data being stored in China. TikTok Ireland informed the DPC that statements it had made to the DPC during the Inquiry regarding its storage of EEA User Data in China were incorrect. TikTok Ireland subsequently informed the DPC that storage of some EEA User Data occurred on two types of databases in China.

111. The DPC became aware of these issues on 9 April 2025, only after the four week period referred to in Article 60(4) GDPR concluded on 21 March 2025. While TikTok Ireland informed the DPC, on the same date as the deadline of that four week period, that matters had come to its attention which will require the correction and/or clarification of statements previously made to the Inquiry, TikTok Ireland did not provide further information at that point.

112. Accordingly, the scope of the DPC's Preliminary Draft Decision and the DPC's Draft Decision considered TikTok Ireland's transfers of EEA User Data only insofar as those transfers consisted of remote access to EEA User Data in China by personnel of affiliate companies of TikTok Ireland who are located in China and are part of the ByteDance group of companies ('**the China Group Entities**'). The scope of the DPC's Preliminary Draft

Decision and the DPC's Draft Decision did not consider TikTok Ireland's transfers of EEA User Data that resulted in that personal data being stored on servers in China.

113. The material scope of this Decision also concerns the transfer of EEA User Data to China under the 2010 SCCs and the 2021 SCCs insofar as those transfers occurred by means of remote access to EEA User Data stored on servers outside of China ('**the Data Transfers**'). Accordingly, where this Decision refers to *"the Data Transfers"*, unless otherwise indicated, this refers to the transfers that occurred by means of remote access to EEA User Data stored on servers outside of China, and does not refer to TikTok Ireland's transfers that resulted in EEA User Data being stored on servers in China.

114. While TikTok Ireland's transfers of EEA User Data to China resulting in the storage of that personal data on servers in China falls outside the material scope of this Decision, the DPC reiterates to TikTok Ireland its deep concern that TikTok Ireland submitted inaccurate information to the Inquiry regarding its transfers. As a result of this inaccurate information, the DPC's consideration of TikTok Ireland's transfers of personal data to China in the Inquiry has been limited to the transfers occurring by means of remote access and the Inquiry has been prevented from investigating all of TikTok Ireland's transfers of EEA User Data to China.

115. The DPC notes TikTok Ireland's position that the issue leading to EEA User Data being stored in China occurred in *"limited cases"* and that TikTok Ireland conducted a *"prompt and extensive investigation"* upon discovery of the issue. The DPC also notes TikTok Ireland's position that it migrated the relevant data from China to Singapore on 21 March 2025, and that it permanently deleted the data in China on 26 March 2025. Nonetheless, the DPC takes this issue very seriously and will continue to engage with TikTok Ireland on these issues, using all necessary and appropriate regulatory powers, in consultation with its peer EU regulators.

116. The Inquiry is concerned with the Data Transfers taking place from 29 July 2020 and ongoing until 17 May 2023, the date of the Preliminary Draft Decision (**'the temporal scope'**).

b) Issues

117. The following issues arise for determination in the Inquiry:

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 and the 2021 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 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 Articles 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 law and practices in effect in China, and whether, and extent to which, there is a risk that the 2010 SCCs and the 2021 SCCs were 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.

3) 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 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)(c) GDPR, so that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within EU.

4) 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.

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 provided to EEA users of the TikTok platform concerning the transfers the subject of the Inquiry.

118. Although the Statement of Issues in the Inquiry made reference exclusively to the 2010 SCCs, further to the letters exchanged by the DPC and TikTok Ireland dated 3 October 2022 and 23 October 2022, the scope of the Inquiry includes a consideration of the above Issues as they concern the 2021 SCCs, in light of TikTok Ireland's Submission dated 19 December 2022.

E. Issue 1 – Transfers and Reliance on the 2010 SCCs and the 2021 SCCs

119. In this section of the Decision, 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 and the 2021 SCCs in connection with the Data Transfers.

a) Overview of transfers under the 2010 SCCs and the 2021 SCCs

120. The Data Transfers considered in this Inquiry concern remote access to EEA User Data in China by personnel of affiliate companies of TikTok Ireland who are located in China and are part of the ByteDance group of companies ('**the China Group Entities**').

121. The concept of a *"transfer to a third country*" is not defined in the GDPR.[24] 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*."[25] The EDPB has also clarified that:

> It should be kept in mind that remote access from a third country (even if it takes place only by means of displaying personal data on a screen, for example in support situations, troubleshooting or for administration purposes) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer, provided that the three criteria outlined in paragraph 9 above are met.[26]

122. It is clear that remote access to EEA User Data by personnel of the China Group Entities working in China falls within the concept of a *"transfer"* for the purpose of Chapter V of the GDPR.

123. TikTok submitted in its Submission dated 15 September 2022 that Issue 1 is unclear.[27] The DPC does not agree with the suggestion that Issue 1 is unclear or that any alleged lack of clarity has deprived TikTok Ireland of the opportunity to make meaningful submissions in response to this Issue. It is necessary, in the context of the Inquiry, for the DPC to obtain and assess information to make findings concerning the relevant facts that underpin the context for the legal assessment of the transfers the subject of the Inquiry. Issue 1 is, as stated, directed to the relevant facts as to TikTok Ireland's reliance on the 2010 SCCs and the 2021 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. A summary of the relevant key facts and the DPC's conclusions in respect of same are set out below.

124. The relevant features of the transfers under the 2010 SCCs and the 2021 SCCs are summarised below.

125. The Data Transfers subject to this Inquiry have undergone various sets of changes since the commencement of the Inquiry on 14 September 2021. As set out above, TikTok Ireland provided the DPC with five Data Transfer Assessments during the Inquiry, which reflect how matters relevant to the transfers have been subject to ongoing changes since the commencement of the Inquiry:

---

[24] Nor was the expression previously defined in Directive 95/46/EC, see judgment of the CJEU of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, at paragraph 56.
[25] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021), at pages 10 and 11.
[26] European Data Protection Board (EDPB), Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (14 February 2023), at page 8
[27] TikTok Ireland's Response dated 15 September 2022, at pages 3 - 4.

(i) Data Transfer Assessment dated 12 October 2021 relating to transfers under the 2010 SCCs,

(ii) Data Transfer Assessment dated 13 October 2022 relating to transfers under the 2010 SCCs,

(iii) Data Transfer Assessment dated 19 December 2022 relating to transfers under the 2021 SCCs,

(iv) Data Transfer Assessment dated "October 2023" relating to transfers under the 2021 SCCs,

(v) Data Transfer Assessment dated "July 2024" relating to transfers under the 2021 SCCs.

126. The ongoing changes since the commencement of the Inquiry include, amongst others, TikTok Ireland's transition to the 2021 SCCs during the scope of the Inquiry, developments in Chinese law and practices, changes to the China Group Entities, and changes in supplementary measures put in place by TikTok Ireland. Furthermore, during the course of the inquiry, TikTok Ireland notified the DPC that it had begun designing and implementing Project Clover.

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.

i. TikTok Ireland's submissions on the storage of personal data of EEA users on servers outside of China under the 2010 SCCs

128. TikTok Ireland informed the DPC that under the 2010 SCCs, personal data of EEA users of TikTok was not stored on servers in China.[28] TikTok Ireland stated that EEA User Data was stored on servers in data centres located in Singapore and the United States[29] which are, respectively, owned and operated by TikTok Pte. Limited and TikTok Inc.[30] TikTok Ireland stated that EEA User Data was also hosted by external cloud providers located outside of China.[31] While TikTok Ireland informed the DPC on 9 April 2025 of an issue that resulted in some EEA User Data being stored on servers in China during the temporal scope of the Inquiry, as set out above, those transfers fall outside the material scope of this Decision.

129. TikTok Ireland's position was that its remote access solution used by the China Group Entities to access EEA User Data does not result in the storage, in any form, of that personal data in China.[32] TikTok Ireland emphasised in its submissions that the storage of personal data on servers outside of China, and, in TikTok's submission, outside of the territorial jurisdiction of the Chinese authorities, is an "*overarching and important*

[28] TikTok Ireland's Response dated 12 October 2021, at pages 19 and 20.
[29] TikTok Ireland's Response dated 12 October 2021, at pages 1, 2 and 3.
[30] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 32 and 34, Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 61.
[31] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 32, 35, 36. TikTok Ireland's Response dated 12 October 2021, at pages 6 and 7.
[32] TikTok Ireland's Submission dated 11 March 2024, at page 12.

fact" to which the DPC ought to have due regard.[33] TikTok cited the Oxford English Dictionary and Collins Dictionary definitions of *"storage"*[34] in support of its position that the processing of personal data by means of the Remote Access Solution does not result in storage of that personal data in China because it does not provide a location for data when it is not being used, so that it can be later retrieved for any purpose.

130. However, the Remote Access Solution results in EEA User Data being temporarily processed on computer information systems in China. Such processing on local devices is implicit in any remote access solution and is an inevitable consequence of any remote access solution. TikTok Ireland accepts that the China Group Entities' use of the Remote Access Solution is a transfer to China for the purposes of Chapter V of the GDPR. TikTok Ireland also accepts that the Remote Access Solution results in the personal data of EEA users being processed in China for the purposes of Article 4 GDPR.[35]

131. In its Response dated 12 October 2021, TikTok Ireland outlined as follows:

> 12.1 EEA User Data is stored in data centres in the US (State of Virginia) and Singapore. The precise flow of data to and from these data centres depends on the nature of the data transmitted.
>
> 12.2 In particular, EEA User video content is first transmitted over [redacted] to "edge data centres" in Europe. The infrastructure for edge data centres is provided by [redacted] and [redacted] This proximate storage enables users to benefit from enhanced video upload performance. This video content is then transmitted over [redacted] to the data centre in Virginia, United States ("Virginia Data Centre"). Video content is stored in the Virginia Data Centre and is currently not mirrored in the data centre in Singapore.
>
> [redacted][36]

132. An examination of transfers of EEA User Data to Singapore and the United States falls outside the scope of this Inquiry. An examination of transfers of personal data of EEA users to Malaysia also falls outside the scope of this Inquiry (as set out in this next subsection of this Decision regarding the question of storage following the implementation of the 2021 SCCs). The processing of EEA User Data in those third countries is outlined

[33] TikTok Ireland's Submission dated 15 September 2022, at page 13.
[34] "(i) the Oxford English Dictionary "the action of storing or laying up in reserve" or store "a stock of anything… laid up for future use"; (ii) Collins Dictionary "If you refer to the storage of something, you mean that it is kept in a special place until it is needed"."
[35] Article 4 defines 'processing' as 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.
[36] TikTok Ireland's Response dated 12 October 2021, at page 16.

here solely insofar as it forms part of the necessary background and context for the transfer of EEA User Data to China.

133. TikTok Ireland has named [redacted] and [redacted] as processors which act as external cloud providers on behalf of TikTok Ireland in the EU and the US, and refers to the security measures, including ISO and SOC I, SOC II and SOC III certifications, which apply to those external cloud providers.

134. TikTok Ireland further states that TikTok Pte. Limited, which owns and operates servers in Singapore, and TikTok Inc., which owns and operates servers in the US, each hold ISO 27001 certifications.[37]

ii. TikTok Ireland's submissions on the storage of personal data of EEA users on servers outside of China following TikTok Ireland's implementation of the 2021 SCCs

135. Under the 2021 SCCs, TikTok Ireland submitted that it remained the position that EEA User Data was stored on servers located in Singapore and the US[38], and was not stored on servers in China. On 28 March 2023, TikTok Ireland wrote to the DPC with a summary of upcoming changes to its EEA Privacy Policy, including to accommodate data storage in its Malaysia data centre and updates to add Malaysia to the list of countries where its servers are located.

136. The information regarding the certifications held by TikTok Pte. Limited, which owns and operates servers in Singapore, and TikTok Inc., which owns and operates servers in the US, in certifications of external cloud providers in the EU and US including [redacted] and [redacted], was reiterated in TikTok Ireland's Data Transfer Assessment dated 19 December 2022 relating to the 2021 SCCs.

137. As set out above, contrary to TikTok Ireland's earlier position, some EEA User Data was in fact stored on servers in China during the temporal scope and, according to TikTok Ireland, up to 26 March 2025. The material scope of this Decision concerns transfers that occurred by means of remote access to EEA User Data stored on servers outside of China. Therefore, transfers resulting in the storage of EEA User Data in China fall outside the material scope of this Decision.

iii. Remote access by personnel of the China Group Entities under the 2010 SCCs

138. As set out above, the relevant transfers of EEA User Data to China under the 2010 SCCs for the purposes of this Inquiry concerned transfers in the form of remote access to EEA User Data by personnel of the China Group Entities.[39]

---

[37] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 32–33. Data Transfer Assessment – China Group Entities dated 13 October 2022, at pages 61–62.
[38] Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 2 and 8
[39] TikTok Ireland's Response dated 12 October 2021, at page 2. See also Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 1, 4, and 30, Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 5. TikTok Ireland's Submission dated 15 September 2022, at page 4, fn. 5.

139. At Appendix A to TikTok Ireland's Data Transfer Assessment dated 12 October 2021, a list of 26 companies identified as the China Group Entities was provided to the DPC. TikTok Ireland noted that "*this list may change from time to time depending on business needs*."[40]

140. At Appendix A to TikTok Ireland's Data Transfer Assessment dated 13 October 2022, an updated list was provided comprising 16 companies identified as the China Group Entities.

141. The China Group Entities were described as acting as processors within the meaning of Article 4(8) GDPR on behalf of TikTok Ireland.[41]

142. In response to a query by the DPC, TikTok Ireland stated that the access granted to the China Group Entities to EEA User Data was limited to remote access, and no third party sub-processor engaged by China Group Entities had a role in processing such EEA User Data. TikTok Ireland stated that the China Group Entities did not transfer the EEA User Data arising from or connected with the Transfers to third party sub-processors.[42]

143. TikTok Ireland outlined that permissions for remote access to limited EEA User Data were granted on a case-by-case basis to certain staff of the China Group Entities, in their capacity as service providers and processors or sub-processors on behalf of TikTok.[43]

144. The nature of the remote access was explained by TikTok Ireland as follows:

> Where access to EEA User data is required to support TikTok, personnel in China must remotely access the data as the data is stored on servers outside of China. Steps are taken to ensure that such remote access is restricted and limited; there is a robust data access management framework in place to ensure: (i) there is restricted and limited access to a data set; (ii) access approval is only granted where appropriate and on a "least privileged" basis; (iii) strong authentication measures and logging of access is in place; and (iv) access is time limited. […][44]

145. It further outlined that:

> TikTok has developed a set of internal web-based tools to control remote access to EEA User Data, including access by our internal support services in China. […] [redacted] system, is integrated with all internal systems to authenticate, authorise and audit access to EEA User Data. Permissions are granted based on the concept of least privilege, allowing only the necessary access for employees to accomplish their job function. Employees requesting access to data must submit a data authority application, which follows a defined approval workflow based on the sensitivity of the requested application or data.[45]

146. It further explained that:

---

[40] TikTok Ireland's Response dated 12 October 2021, at pages 3.
[41] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 1 and 4.
[42] TikTok Ireland's Response dated 20 June 2022, at page 4.
[43] Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 2 and 8.
[44] TikTok Ireland's Response dated 12 October 2021, at page 7.
[45] TikTok Ireland's Response dated 12 October 2021, at page 16.

In technical terms, in order to actually gain access to the particular resource, the relevant employee must:

(1) successfully log in [redacted];

(2) be connected to the [redacted] network [redacted]; and

(3) sign into the particular application or database containing the resource [redacted].[46]

147. The more detailed features of the above are considered further below under Issue 3 (Supplementary Measures).

148. TikTok Ireland also indicated that the duration of specific remote access authorised was generally limited to no more than 12 months.

149. Remote access was not authorised at the entity level (there was no authorisation that extended to all personnel within a China Group Entity regardless of role or function). Where remote access was authorised, only personnel within a particular China Group Entity who, based upon the business need for their role or function to access the data, were covered by the particular authorisation were to be given remote access. Such personnel were not given access to the full range of personal data of a particular user.[47]

150. TikTok Ireland provided the DPC with certain documented policies and procedures relevant to the remote access concerned by the transfers the subject of the Inquiry, which are considered further below under the section of this Decision concerning supplementary measures.[48]

iv. Remote access by personnel of the China Group Entities following TikTok Ireland's implementation of the 2021 SCCs

151. TikTok Ireland stated that a "*reorganisation*" took place resulting in what were previously direct transfers to certain China Group Entities being made to them indirectly (onward), in accordance with Clause 9(b) of the SCCs, via one of the China Group Entities.

152. A list of the 16 China Group Entities to whom direct transfers and indirect (onward) transfers were made was given in Appendix A to TikTok Ireland's Data Transfer Assessment dated 19 December 2022. The list of companies is the same as the list given in Appendix A to TikTok Ireland's Data Transfer Assessment dated 13 October 2022, save for a change of name in respect of two of the companies.

153. The initial transfer was made to Beijing Zitiao Network Technology Co., Ltd. and onward transfers were made by it to 15 further China Group Entities.[49] TikTok Ireland has clarified that whereas, prior to the reorganisation, TikTok, under the 2020 Intra-Group Agreement, engaged each of the China Group Entities directly and entered into 2010 SCCs with each China Group Entity, in the context of the reorganisation that took place

[46] TikTok Ireland's Response dated 20 June 2022, at page 5.
[47] TikTok Ireland's Response dated 20 June 2022, at pages 5, 6 and 7.
[48] These included [redacted]
[49] Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 8.

under 2021 SCCs, TikTok Ireland engaged only Beijing Zitiao Network Technology Co., Ltd. ('**the Primary Processor**') directly, and the Primary Processor then separately engaged each of the other China Group Entities ('**the Subprocessors**'). It outlined that this resulted in a streamlining of the process whereby a single entity, the Primary Processor, had contractual responsibility as the Primary Processor to TikTok Ireland for all the processing services provided by the Subprocessors.[50] These arrangements are reflected in the updated European Transfer Matrix.

154. The processing chain under the 2021 SCCs remained limited to the China Group Entities.

155. Further, TikTok Ireland stated that the technical and organisational measures applicable to these transfers (including the controls around the means by which remote access is granted) prior to the reorganisation continued to apply following the reorganisation, as reflected in the Data Transfer Assessment dated 19 December 2022.

156. The purpose of the update was to clarify the application of certain principles and to clarify how approvals/authority should be managed. This included allowing for Business Leaders to delegate or escalate matters in certain cases, introducing rules regarding cross-regional authority applications in certain cases, where the permission recipient's work location is different to the region of the user's personal information (e.g. a permission recipient located in China requesting access approval for EEA User Data), and reflecting changes in certain roles, such as the role of the Global Security Organisation (GSO) in approving applications with respect to data concerning users from Europe and the US.

v. Purposes for which the personal data was remotely accessed under the 2010 SCCs

157. The purposes for which the personal data of users of the TikTok platform was transferred to the China Group Entities under the 2010 SCCs were described in Appendix B to each of the Data Transfer Assessments dated 12 October 2021 and 13 October 2022.

158. The version of Appendix B included with the Data Transfer Assessment dated 13 October 2022 contained some updates compared with the previous version, and it is that updated version which is set out below.

Roles of Authorised Personnel	Related processing purposes
Trust & Safety	
[redacted]	▪ To manage and provide technical support in developing, testing, maintaining and optimising Trust & Safety features (e.g. functionality, tools, and systems). ▪ To evaluate and monitor performance metrics of Trust & Safety features, and to measure their effectiveness. ▪ To review and evaluate the quality of tools and processes. ▪ To provide limited Trust & Safety Operations support (e.g. triaging content reports and/or user feedback for escalation to relevant teams).
TikTok Product	

[50] TikTok Ireland's Response dated 28 March 2023, at pages 1–2.

[redacted]	▪ To evaluate and monitor core performance metrics across the TikTok Platform. ▪ To develop, test, maintain and optimise the Platform and product features. ▪ Trouble-shooting and debugging of technical and performance issues (e.g. where the application is crashing / not responding). ▪ To address account performance issues.
Product Monetisation	
[redacted]	▪ To develop, test, maintain and optimise advertising products and models, and to evaluate and optimise advertising effectiveness and performance. ▪ Develop, test, maintain and optimise tools for advertising integrity and brand safety. ▪ Support in relation to the TikTok Creator Marketplace and Creator Fund.
Online Payments	
[redacted]	▪ To protect the Platform from fraudulent payments, deal with chargeback queries from merchant banks and for financial regulation compliance purposes. ▪ To address customer queries relating to transactions they have made on the Platform.
Global Information Security	
[redacted]	▪ Testing and monitoring security measures and risks ▪ Debugging and trouble-shooting bugs and identified vulnerabilities and patching of technical issues. ▪ Incident investigation, containment, mitigation and remediation, and incident reports. ▪ Handling and investigating vulnerabilities reported by users / third parties.

159. In response to a query by the DPC, TikTok outlined that:

> TikTok shares information with personnel within the China Group Entities as necessary to enable them to provide important functions such as research and development, security, analytics, online payments, and customer and technical support. While many of these functions are also performed by teams in Europe and in other countries, TikTok also relies on the personnel within the China Group Entities in order to ensure the development and maintenance of TikTok's Platform and 24/7 customer support to the EEA Users who use the TikTok Platform.

Remote access to specific resources is to be granted to personnel in a China Group Entity based upon a legitimate business need for the role or function to access that data.[51]

160. It is clarified that *"[r]esources in this context generally means an application (or certain functionality in an application) or a database. EEA User Data is contained in these resources. It is important to note that not all applications or databases used in TikTok contain EEA User Data."*[52]

vi. Purposes for which the personal data was remotely accessed following TikTok Ireland's implementation of the 2021 SCCs

161. Appendix B to the Data Transfer Assessment dated 19 December 2022 refers to the European Transfer Matrix[53] in respect of the purposes for the processing. The processing purposes are represented in the European Transfer Matrix by reference to (i) the nature of the processing and (ii) the purpose of the processing, and are set out specifically by reference to each of the 16 China Group Entities that receive a direct or indirect (onward) transfer of EEA user data.

162. An illustrative extract from the European Data Transfer Matrix in this regard is the following, which concerns the initial transfer from TikTok Technology Limited to Beijing Zitiao Network Technology Co., Ltd.

Row 4, Column I – Nature of processing
▪ Troubleshooting using engineering metrics or logs related to a specific user or, where necessary to fix the problem, specific user data. ▪ Fixing issues in the production system and validating that the issue has been successfully remediated. ▪ Viewing aggregated A/B testing results. ▪ Testing new tools, platforms and systems to ensure they work correctly in a live environment. ▪ Analysing certain data such as reported user cases, account information, device information, behaviour logs, payment & transaction information to identify suspicious and malicious behaviours and preventative models and tooling to combat these behaviours on the Platform. ▪ Developing, testing, maintaining and optimising machine learning models and algorithms. ▪ Reviewing customer feedback tickets to understand the nature of specific technical issues, triaging these issues, routing to the appropriate engineering (or payment) team if necessary. ▪ Analysing aggregated business or technical metrics such as daily active users, daily new users, user growth, product feature engagement, and ads engagement. ▪ Reviewing stats of top creators to support these creators in developing their profile on the Platform. ▪ Building aggregated dashboards for business teams.

[51] TikTok Ireland's Response dated 20 June 2022, at page 5.
[52] TikTok Ireland's Response dated 20 June 2022, at page 5.
[53] TikTok Ireland's Submissions dated 19 December 2022, Schedule, Document 4.

▪ To protect the Platform from fraudulent payments, deal with chargeback queries from merchant banks and for financial regulation compliance purposes. ▪ Monitoring and evaluating content trends to ensure the effectiveness of Trust & Safety tools and strategies. ▪ Investigating moderation outputs in suspected cases of moderator misconduct. ▪ Reviewing of moderation outputs to determine how overall efficiencies and effectiveness can be improved, and for capacity and training purposes.
Row 4, Column J – Purpose of processing
Content delivery, security, research and development, analytics, online payments, customer and technical support, and content moderation.

163. Processing and processing purposes of a similar nature are outlined in respect of each of the other 15 China Group Entities which received indirect (onward) transfers in the context of the transfers under the 2021 SCCs.

vii. Categories of personal data the subject of remote access under the 2010 SCCs

164. TikTok Ireland provided an outline of the categories of the personal data of EEA users of the TikTok platform the subject of transfers to the China Group Entities in Appendix C to the Data Transfer Assessments dated 12 October 2021 and 13 October 2022.

165. As above, the version of Appendix C included with the Data Transfer Assessment dated 13 October 2022 contained some updates compared with the previous version, and it is the information in that updated version which is set out below.

User ID and TikTok username	A TikTok User ID is a number linked to each TikTok account and used for internal operational purposes. User ID does not appear on the face of a user's profile (but can be accessed by each user in-app). A TikTok username (or nickname) is the name that a user chooses when they create a TikTok profile (not to be confused with a user's actual name). TikTok username is shown on the user's profile page in the following format: "@xxxxxx", and can be changed by the user at any time.
Subscriber data	This is the data that a user provides or which is generated by TikTok when a user registers on the Platform. In addition to username, it includes: email address and/or phone number (depending on user's sign-up method), date of birth, account creation date, IP address at account creation, device information and country-of-registration.
User profile	This is information that a user chooses to disclose in their profile, which in addition to username, may (optionally) include: a profile photo, bio statement, gender, and handles for other social platforms (such as Instagram and/or YouTube).
Interaction / activity data	These are data points on a user's engagement on the Platform, which are generally linked to a User ID, such as customer support archives, number of followers, number of views for videos posted, number of videos liked, number of videos shared and other similar activity.
Content data	This is user generated content, including video content, audio files, comments and direct message content. Each video also has a video identifier (i.e. similar to User ID but for each video).
Technical and advertising related data	This category of data includes device data (e.g. Mobile Advertising ID, device model, operating system etc.), network data (e.g. network carrier, connection type, IP address, etc.), transaction data, coarse location, interest category selection (e.g. comedy, animals, sports,

	etc.), inferred demographic and interest profiles (based on device data/network data and interaction/activity data), ad and off app engagement data (e.g. event parameters regarding users' in-app or off-app interaction with advertising content).
Purchase Information	This category includes transaction information (such as payment type, account balance, transaction ID) and purchase history.

166. TikTok Ireland indicated that "*TikTok does not specifically collect special category data from EEA Users*".[54] It is stated in respect of users of ByteDance apps, products and services at Schedule [redacted] of the 2020 Intra-Group Agreement that [redacted]

167. In response to a query by the DPC, TikTok Ireland stated that the processing by the China Group Entities of EEA user data "*is not for the purposes of revealing or deducing*" special category data of EEA users under Article 9 GDPR or data relating to criminal convictions or offences under Article 10 GDPR. It clarified that "*[d]epending on the context of the processing, personal data which could potentially be capable of revealing [special category data] may be processed incidentally by TikTok or uploaded by EEA Users on the Platform. However, as stated, the processing undertaken by the China Group Entities in respect of EEA User Data is not for the purposes of revealing or deducing [special category data]*".[55]

viii. Categories of personal data the subject of remote access following TikTok Ireland's implementation of the 2021 SCCs

168. By way of illustration, a representative extract from the European Data Transfer Matrix in this regard is the following, which concerns the initial transfer from TikTok Technology Limited to Beijing Zitiao Network Technology Co., Ltd.

Row 4, Column F – Categories / Type of personal data
Personal data relating to TikTok Users in the EEA/CH which is transferred to the ByteDance Transferee which can include External Device Identifiers, First Party Identifiers, Real Life Identifier & Info, Account Profile, Login and Registration, Account, System Info, Mobile Carrier Info, App Info, Location, Device Info, Network Info, Notification, Ads Data, UGC, Payment Info, Transaction and Balance, Survey Responses, User Behaviour Data, User Support and User Requests.

169. A Data Category Key is included at a separate sheet of the EEA Data Transfer Matrix.

170. The Data Category Key further explains each of the data categories listed above as follows:

Data Category Key	
External Device Identifier	such as IP, IDFA, IDFV, Android ID, GAID, and Advertising ID.
First Party Identifier	such as User ID, Device ID, Video ID, Entity ID (inc Comment ID and message ID), Item ID, Music ID, Order ID.
Real Life Identifier & Information	such as Real Name, Address, Nationality, email, phone number, birthdate, age, gender and postcode.
Account Profile	such as profile image, profile bio, in-app name, third party profile (if shared).
UGC	user generated content such as video, image, audio, text, UGC metadata, UGC list.

[54] TikTok Ireland's Response dated 12 October 2021, at page 1.
[55] TikTok Ireland's Response dated 20 June 2022, at page 4.

User Support and User Requests	such as user support requests and data subject requests.
Login and Registration	such as login source and information and login session and token.
System Info	such as operating system, user agent, and system settings.
Mobile Carrier Info	such as carrier info, MCC and MNC, and cell Info.
Account or Content Tag	such as content labels applied by moderators or machine learning models.
App Info	App Info such as App version, App ID, App Name, App Release /Download Channel, App Install ID, App Package Name.
Device Info	such as language, device brand and model, screen density and resolution.
Network Info	such as network access mode, Wi-Fi related info, and network bandwidth.
Ads data	such as Ad campaign conversion, mobile attribution, DMP and data provided by Advertisers.
Notification	such as push notifications sent to users.
Location	such as country / region / city (including system language and region), or approximate location based on GPS (if chosen by the user).
Payment Information	such as bank account, BIN, and payment authentication token.
Transaction and Balance	such as transaction history and virtual assets.
Survey Responses	such as responses from users who respond to surveys.

171. A similar range of categories of personal data of EEA users the subject of the remote access were outlined in respect of the other 15 China Group Entities which receive indirect (onward) transfers in the context of the transfers under the 2021 SCCs.

172. Similar to the position expressed by TikTok Ireland in respect of the transfers under the 2010 SCCs, TikTok indicates in the European Transfer Matrix that *"[i]t is generally not the intention of TikTok to collect any Sensitive Data, however Sensitive Data may be collected incidentally or uploaded by the User*."

173. "*Sensitive data"* is defined in the General Definitions to the European Transfer Matrix to mean *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences*." The definition in substance corresponds to the definitions of special categories of personal data and personal data relating to criminal convictions and offences under Articles 9 and 10 GDPR.[56]

174. In response to the Preliminary Draft Decision, TikTok Ireland stated that, while TikTok Ireland does not operate a real name policy, personal data including a user's real name, address, and postcode are required in specific cases including for payment services, for age verification purposes as part of the underage appeals process, and *"when popular creators wish to host LIVE sessions on TikTok…"*.

[56] Article 10 GDPR limits the processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) to the control of official authority or where authorised by EU/ Member State law with appropriate safeguards for rights.

175. TikTok Ireland also confirmed that, while it did not collect precise location information about EEA Users, it did collect users' location at country or city level, and it did collect approximate location information with consent in some instances (accurate to an areas of 3 square kilometres).

ix. Format of personal data remotely accessed under the 2010 SCCs

176. It was recorded in the Data Transfer Assessments dated 12 October 2021 and 13 October 2022 that the format of the personal data the subject of the transfer remotely accessed by the China Group Entities would be [redacted][57]

177. TikTok Ireland has further outlined that:

> [b]ased on demonstrated need (such as the investigation of security incidents), authorised personnel within China Group Entities can request the ability to see decrypted data elements. It is technically not possible to decrypt this encrypted user data without a key that has been generated and managed by [redacted][58]

178. In a query by the DPC, TikTok Ireland was requested to give a full account of the circumstances in which personnel of the China Group Entities may require remote access to unencrypted, decrypted, or plain-text data of EEA users for the purposes set out in Appendix B of the Data Transfer Assessment, or for any other purpose, and, further, to clarify the procedures relating to, and oversight of, access to unencrypted, decrypted or plain-text data of EEA users.

179. TikTok Ireland referred to the information given in the part of its response quoted above with regard to authorisation of access to resources based on business needs, and indicated that where an employee needed access to a particular resource that contained encrypted data based upon a business need, the employee would be given remote access to the encrypted data in unencrypted form provided the access was approved through the approval process.[59]

180. TikTok Ireland further clarified that *"[t]here is no additional standalone policy, procedure, rules or frameworks regulating requests for decrypted, encrypted or plain text data. Rather, the approval process for these requests is regulated in accordance with TikTok's general access permission processes and is subject to the same oversight*."[60]

181. TikTok Ireland additionally outlined in its Submission dated 15 September 2022 in response to the Statement of Issues that:

> With regard to paragraphs 39 and 40 of the Statement of Issues, TikTok would like to clarify that, where an individual working for a China Group Entity requests access to an application (or certain functionality in an application), and access to that application is considered to be required for the individual's particular role, the individual will, upon approval through the approval process, be given remote access to the application. This includes access, in unencrypted form, to encrypted data

[57] Data Transfer Assessment – China Group Entities dated 12 October 2021, at page 4 and Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 5.
[58] TikTok Ireland's Response dated 12 October 2021, at page 9, and in Section 3 of the Data Transfer Assessment dated 12 October 2021, at page 28.
[59] TikTok Ireland's Response dated 20 June 2022, at page 15.
[60] TikTok Ireland's Response dated 20 June 2022, at page 15.

accessible through that application. This reflects that the relevant applications can only be properly accessed in the manner for which there was judged to be a valid and approved need where the data is accessible in unencrypted form.

However, where the individual originally requests access to a database which contains encrypted data, the grant of approval to access the database does not result in the individual getting access to the encrypted data within the database in unencrypted form. The individual must, through the approval process, obtain a separate permission to get access to encrypted data contained within the database. If the individual demonstrates a valid need, they will be given access to the data in unencrypted form through this additional approval process. This reflects that it is not in all cases necessary to be able to access, in unencrypted form, the encrypted data contained within a particular database.[61]

x. Format of personal data remotely accessed following TikTok Ireland's implementation of the 2021 SCCs

182. The position remained similar in the context of the transfers under the 2021 SCCs. TikTok Ireland's Data Transfer Assessment dated 19 December 2022 records that the format of the personal data the subject of the remote access would be "*Encrypted / Pseudonymised / Plain-text*".[62] It was again outlined that personnel of China Group Entities were given authorised remote access to EEA User Data in, as applicable, encrypted, plain text or pseudonymised form where their role required remote access to this type of data and access to it fell within the scope of an approval given.[63]

xi. Sharing of data for use in other ByteDance products

183. In its request for further information dated 11 May 2022, at Query II(5), the DPC noted that the [redacted]

184. The DPC asked TikTok Ireland to identify the situations in which data sharing between products such as Toutiao, TikTok, Douyin or any other ByteDance product may occur and to state whether such data sharing involves or may involve personal data of EEA users.

185. In response to that query, TikTok Ireland stated that TikTok did not share EEA User Data with other ByteDance companies in China for use in other ByteDance products (including Toutiao and Douyin).[65]

186. It further stated that:

> Users from TikTok and Douyin (and other ByteDance Chinese products and services) cannot interact with each other across the services.

---

[61] TikTok Ireland's Submission dated 15 September 2022, at page 20, fn. 50.
[62] TikTok Ireland's Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 8.
[63] TikTok Ireland's Submission dated 19 December 2022, inter alia, at page 67.
[64] TikTok Ireland's Response dated 12 October 2021, Appendix A, Document 8.
[65] TikTok Ireland's Response dated 20 June 2022, at page 8.

Further, due to geographical, technical and infrastructural segregation, there is no possibility of intermingling of EEA User Data (which is stored outside China) with Douyin user data (which is stored in China).[66]

xii. Reliance on the 2010 SCCs as the relevant transfer tool

187. TikTok has confirmed, for purposes prior to December 2022, that the only relevant transfer tool for the purpose of Chapter V GDPR it relied on as an appropriate safeguard when permitting authorised remote access to personal data of EEA users by personnel located in China were SCCs under Article 46(2)(c) GDPR, together with supplementary measures.[67]

188. TikTok Ireland and the China Group Entities were, prior to December 2022, party to an Intra-Group Data Agreement for Transfers of Personal Data between ByteDance Entities dated 29 July 2020 ('**the 2020 Intra-Group Agreement**').

189. [redacted]

190. [redacted]

[redacted]

191. [redacted]

[redacted]

192. [redacted]

[66] TikTok Ireland's Response dated 20 June 2022, at page 3.
[67] TikTok Ireland's Response dated 12 October 2021, at page 2. See also Submissions dated 15 September 2022, at page 4.

193. [redacted]

194. [redacted]

195. As set out above, the China Group Entities were described as acting as processors on behalf of TikTok Ireland.

196. [redacted]

[redacted]

197. [redacted]

198. [redacted]

199. [redacted]

200. TikTok Ireland has provided a copy of the description of the technical and organisational measures set out in [redacted] of the Intra-Group Agreement which are deemed to be inserted in place of Appendix 2 to the 2010 SCCs.[74]

201. [redacted]

[redacted]

[74] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 2.

[redacted]

202. [redacted]

xiii. Reliance on the 2021 SCCs as the relevant transfer tool

203. As set out above, during the course of the Inquiry, TikTok Ireland made a transition from the 2010 SCCs to the 2021 SCCs in advance of the deadline of 27 December 2022 stipulated in Article 4(4) of European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

204. TikTok Ireland entered into a new Intra-Group Agreement ('**the 2022 Intra-Group Agreement**') to implement the 2021 SCCs with effect from 19 December 2022. TikTok Ireland also put in effect an updated Data Transfer Assessment dated 19 December 2022. The 2022 Intra-Group Agreement regulated transfers of personal data between all entities of the Bytedance group of companies to which TikTok Ireland belongs.

205. TikTok Ireland notified the DPC on 8 September 2023 that it was in the process of updating the 2022 Intra-Group Agreement and that it expected to complete that update by 29 September 2023. However, on 29 September 2023, TikTok Ireland informed the DPC that it had made no changes to the terms of the Intra-Group Agreement. As set out above, TikTok Ireland submitted an updated European Transfer Matrix to the DPC on 6 December 2024, which comprised of updates to the 2022 Intra Group Agreement to reflect updates made as a result of Project Clover. The 2022 Intra Group Agreement remained otherwise unchanged.

206. As TikTok Ireland has stated, the 2022 Intra-Group Agreement was different to the 2020 Intra-Group Agreement, and has provided clarification on the key changes.[75]

207. [redacted]

208. [redacted]

[redacted]

209. [redacted]

210. [redacted]

211. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

212. [redacted]

[redacted]

[redacted]

[75] TikTok Ireland's Submission dated 19 December 2022, at page 4.
[76] TikTok Ireland's Submission dated 19 December 2022, at page 4.

[redacted]

213. [redacted]

214. [redacted]

215. [redacted]

216. [redacted]

[77] TikTok Ireland's Response dated 28 March 2023, at page 1.
[78] TikTok Ireland's Response dated 28 March 2023, at page 1.

217. [redacted]

218. [redacted]

[redacted]

219. [redacted]

220. [redacted]

[redacted]

221. TikTok Ireland has provided the Inquiry a copy of the description of the technical and organisational measures set out in [redacted] of the Intra-Group Agreement.

222. [redacted]

[redacted]

[redacted]

[redacted]

223. [redacted]

[redacted]

224. [redacted]

225. [redacted]

226. [redacted]

b) Findings in Respect of Issue 1

227. The DPC summarises here some of the relevant facts that are core to this Decision's assessment of TikTok Ireland's reliance on the 2010 SCCs and the 2021 SCCs during the temporal scope in connection with the transfers the subject of the Inquiry:

(i) The DPC is 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, the United States and Malaysia during the temporal scope of the Inquiry was a *"transfer"* of personal data for the purposes of

Chapter V of the GDPR. This is not disputed and is supported by the Supplementary Measures Recommendations.

(ii) The DPC notes, regarding the remote access subject to the material scope of this Decision, that the position under the 2010 SCCs and under the 2021 SCCs was that EEA User Data was stored on servers located in Singapore, the United States and Malaysia, and was not itself stored on servers in China. However, this personal data was processed in China further to the Remote Access Solution.

(iii) The DPC is also satisfied that from 29 July 2020 to 19 December 2022, the transfers considered in this Inquiry were made pursuant to the 2020 Intragroup Agreement implementing the 2010 SCCs, and from 19 December onwards, the transfers considered in this Inquiry were made pursuant to the 2022 Intragroup Agreement implementing the 2021 SCCs.

(iv) 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 were 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 sub processors.[79] The processing could have engaged one or more of multiple processors located in China.

(v) The DPC has had regard to the circumstances of the remote access as outlined by TikTok Ireland under both the 2010 SCCs and the 2021 SCCs. In light of both the factual description of the remote access, and the information furnished in respect of the nature of the processing, the DPC finds that the transfers were systematic, repetitive and continuous. The transfers were 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 was authorised for a specific business purpose, it was in general authorised for up to 12 months, a considerable length of time. The purposes for which the transfers were made under the 2010 SCCs, and the 2021 SCCs were 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 have been the subject of the processing were very significant in number. This must be viewed relative to the fact that TikTok is a popular and widely used platform with approximately [redacted] users in the EEA as of May 2022.[80]

(vi) The personal data of EEA users accessed remotely by the China Group Entities may have included sensitive data (aligning broadly to the concept of personal data that may fall within Articles 9 and 10 of the GDPR), despite that the purposes of the services provided by the China Group Entities did not seek to reveal or deduce sensitive data. It may have also included, based on a demonstrated business need, personal data in decrypted or plaintext form.

(vii) Personal data of EEA users of the TikTok platform was not shared with other ByteDance companies in China for use in other ByteDance products (such as Toutiao and Douyin). During the Inquiry, the DPC requested TikTok Ireland, as the data exporter in respect of the Data Transfers, to identify the situations in which data sharing between products such as Toutiao, TikTok, Douyin or any other ByteDance product may occur and state whether such data sharing involves or may involve personal

[79] Zhuhai Juheng Yixing Network Technology Co., Ltd. was added as a new sub processor on 25 June 2023. Hainan Juliang Engine Technology Co., Ltd. and Tianjin Byte Technology Co., Ltd. were removed as sub processors on 1 July 2023.

[80] TikTok Ireland's Response dated 20 June 2022, at page 4.

data of EEA users. TikTok Ireland confirmed that TikTok does not share EEA User Data with other ByteDance companies in China for use in other ByteDance products.

F. Issue 2 – TikTok Ireland's compliance with its obligation to assess the level of protection of personal data of EEA users the subject of the transfers to the China Group Entities using SCCs

a) The legal framework

228. In this this section of the Decision, the DPC will consider whether TikTok Ireland 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.

229. There is an obligation on data controllers making data transfers in reliance on SCCs to first assess the law and practices of the country of destination in the context of the transfers. This assessment is crucial to informing whether the data transfers can proceed on the basis that the personal data will be subject to an essentially equivalent level of protection. This assessment is also crucial to informing the subsequent selection of supplementary measures, where required, in order to verify and guarantee that level of protection.

The Charter

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

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

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

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

234. Article 52 of the Charter recognises that the rights and freedoms recognised by the Charter may be limited, but any such limitation must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, the limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

Chapter V of the GDPR

235. Article 44 GDPR sets out the general principle that transfers of personal data to a third country shall take place only if, subject to the other provisions of the GDPR, the conditions laid down in Chapter V GDPR are complied with by the controller and processor. The provisions in Chapter V are to be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

236. Article 45(1) GDPR provides that a transfer of personal data to a third country may be authorised by decision of the European Commission to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection ('**Adequacy Decision**').

237. China has not been subject of an Adequacy Decision as of the date of this Decision.

238. In the absence of a decision pursuant to Article 45(3) GDPR, Article 46(1) provides that a controller or processor may transfer personal data to a third country 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.

239. Article 46(1) read together with Article 46(2)(c) GDPR indicates that such "*appropriate safeguards*" may be provided, inter alia, by standard data protection clauses ('**SCCs**') adopted by the European Commission.[81]

240. However, having regard to the nature, purpose, and limitations of SCCs adopted on the basis of Article 46(2)(c) of the GDPR in providing guarantees, which are solely a matter of contractual obligation between the controller and the third country recipient to ensure compliance with the level of protection required under EU law, it may be necessary, depending on the prevailing position in a particular third country, for the controller to adopt supplementary measures to ensure that level of protection required under EU is complied with.[82]

The SCCs

241. Decision 2010/87/EU[83] was adopted pursuant to Article 26(4) of Directive 95/56/EC,[84] and, pursuant to Article 46(5) of the GDPR, was stated to remain in effect until amended, replaced or repealed by a Commission Decision adopted in accordance with Article 46(2).

242. Commission Implementing Decision (EU) 2021/914[85] was adopted on 4 June 2021, repealing the 2010 SCC Decision with effect from 27 September 2021, and setting out new SCCs (the 2021 SCCs) which came into effect on 27 June 2021, and which needed to be implemented by controllers and processors by 27 December 2022.

243. Having regard to the temporal scope of the Inquiry, both the 2010 SCCs and the 2021 SCCs are relevant in the present context.

The obligation on controllers and processors to assess the law and practices of the third country, and to verify, guarantee and demonstrate an essentially equivalent level of protection

244. On 6 October 2015, the CJEU delivered its judgment in Case C-362/14 Schrems v Data Protection Commissioner[86] ('**the Schrems I judgment**'). This judgment concerned the validity of an adequacy decision adopted by the European Commission on the basis of Article 25(6) of Directive 95/46. The CJEU set out the requirements stemming from Article 25(6) of the Directive in respect of the European Commission's competence to find that a third country ensures an adequate level of protection:

> As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.

[81] In accordance with the examination procedure referred to in Article 93(2) GDPR.
[82] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 131 and 132.
[83] 2010/87/EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593).
[84] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[85] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
[86] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015 (ECLI:EU:C:2015:650).

However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission 'may find … that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into …, for the protection of the private lives and basic freedoms and rights of individuals'.

It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'.

Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.[87]

245. The Court held that, when examining the level of protection afforded by a third country pursuant to Article 25(6) of that Directive, the European Commission is obliged to assess the content of the applicable rules in

[87] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015 (ECLI:EU:C:2015:650), at paragraphs 68 – 74.

that third country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules. The Court also held that the European Commission is obliged, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified.

246. The Schrems II judgment, delivered on 16 July 2020, concerned, inter alia, the level of protection required in respect of a transfer of personal data to a third country based on standard contractual clauses. In this judgment, the CJEU held that the required level of protection, as in the context of a transfer based on an adequacy decision, is a level of protection essentially equivalent to that which is guaranteed within the European Union:

> As regards the level of protection required, it follows from a combined reading of those provisions that, in the absence of an adequacy decision under Article 45(3) of that regulation, a controller or processor may transfer personal data to a third country 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, such safeguards being able to be provided, inter alia, by the standard data protection clauses adopted by the Commission.
>
> Although Article 46 of the GDPR does not specify the nature of the requirements which flow from that reference to 'appropriate safeguards', 'enforceable rights' and 'effective legal remedies', it should be noted that that article appears in Chapter V of that regulation and, accordingly, must be read in the light of Article 44 of that regulation, entitled 'General principle for transfers', which lays down that 'all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined'. That level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.
>
> As the Advocate General stated in point 117 of his Opinion, the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country, in accordance with the objective set out in recital 6 thereof.
>
> The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph would be undermined (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 73).
>
> In that context, recital 107 of the GDPR states that, where 'a third country, a territory or a specified sector within a third country … no longer ensures an adequate level of data protection. … the transfer of personal data to that third country … should be prohibited, unless the requirements [of that regulation] relating to transfers subject to appropriate safeguards … are fulfilled'. To that effect, recital 108 of the regulation states that, in the absence of an adequacy decision, the appropriate safeguards

to be taken by the controller or processor in accordance with Article 46(1) of the regulation must 'compensate for the lack of data protection in a third country' in order to 'ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union'.

It follows, as the Advocate General stated in point 115 of his Opinion, that such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union.*[88]*

247. Therefore, like in the case of transfers made pursuant to an adequacy decision, transfers made pursuant to Article 46 GDPR must ensure a level of protection essentially equivalent to that which is guaranteed in the European Union. The Court set out the factors that must be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses. Where transfers are conducted under Article 46(1) GDPR, the appropriate safeguards, along with supplementary measures, to be implemented must compensate for any lack of data protection in the third country in order to ensure compliance with data protection requirements and data subjects' rights appropriate to processing within the EU.[89] The judgment makes clear that, in the absence of an adequacy decision, transfers to a third country are permissible only if:[90]

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

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

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

248. Article 46 GDPR requires that the appropriate safeguards, enforceable rights and effective legal remedies required by that article must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter.

249. The CJEU clarified that an assessment of whether, in light of Article 46(1) GDPR, data subjects are afforded appropriate safeguards, enforceable rights and effective legal remedies is required to take into account the following factors:[91]

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

(ii) With regard to 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, considering factors including those set out in Article 45(2) GDPR.

---

[88] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 91 – 96.
[89] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 95 and 131.
[90] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 91 and 103.
[91] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 102–105.

250. As regards any access by public authorities to the personal data transferred, the Court held that the factors to be taken into consideration correspond to those factors, as set out non-exhaustively in Article 45(2) GDPR, that the European Commission must have regard to when assessing the adequacy of the level of protection in the context of an adequacy decision. Article 45(2) GDPR provides:

> When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

251. The CJEU noted that an adequacy decision can be adopted by the European Commission only if the European Commission has found that the third country's relevant legislation ensures an adequate level of protection. In contrast, the CJEU noted, in the case of a European Commission decision adopting standard protection clauses, the European Commission is not required, before adopting such a decision, to assess the adequacy of the level of protection ensured by third countries to which personal data could be transferred pursuant to such clauses. In that context, the CJEU held:

> In that regard, it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject' and that 'those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies … in the Union or in a third country'.
>
> Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, as is clear from paragraph 125 above, but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may

prove necessary to supplement the guarantees contained in those standard data protection clauses. In that regard, recital 109 of the regulation states that 'the possibility for the controller … to use standard data-protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses'.

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.

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.

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.

Therefore, the mere fact that standard data protection clauses in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those in the annex to the SCC Decision, do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of that decision.[92]

252. The Schrems II judgment is clear that, regardless of which appropriate safeguards and supplementary measures a controller or processor chooses to implement, above all, it is for the controller or processor to verify that the personal data transferred to the third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union. In that regard, the CJEU held that the controller or processor established in the European Union must guarantee such protection in light of the additional measures.

[92] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 131 – 136.

253. The Schrems II judgment is also clear that the controller or processor must suspend or end the transfers if it is not able to take adequate additional measures to guarantee that level of protection. Therefore, this obligation to verify and guarantee that the personal data transferred will be subject to an essentially equivalent level of protection rests with the controller or processor. The controller or processor must comply with this obligation before transferring any personal data to a third country and transfers may proceed only if the controller or processor has first verified and guaranteed that the personal data transferred will be subject to an essentially equivalent level of protection.

254. In order to verify and guarantee that the personal data transferred will be subject to an essentially equivalent level of protection, there is an obligation on that controller or processor to first assess the law and practices of the third country in the context of the transfers. This assessment is crucial to informing the level of protection of personal data of data subjects the subject to transfers using SCCs. This assessment must have particular regard to the relevant aspects of the legal system of the third country regarding any access by public authorities of that third country to the personal data transferred. This factor is particularly relevant to the assessment in circumstances where standard contractual clauses cannot bind public authorities. The CJEU has found that, although SCCs are binding on a controller established in the EU and the transfer recipient in the third country, *"those clauses are not capable of binding the authorities of that third country, since they are not party to the contract"*.[93]

255. Consequently, while there are situations in which, depending on the law and practices in force in the third country concerned, the transfer recipient is in a position to guarantee the necessary protection of the data solely on the basis of SCCs, there are other situations in which the content of the SCCs may not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned.[94] Critically, in this respect, the CJEU held that *"[t]hat is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates"*.[95] In that scenario, it may become necessary for the controller to supplement the guarantees contained in the SCCs by other clauses or additional safeguards to *"supplement"* the SCCs, or to adopt further *"supplementary measures"* in order to ensure compliance with the level of protection required under EU law.[96]

256. The purpose of the appropriate safeguards is to compensate for deficiencies in the protection afforded by the third country. If a controller or processor has not clearly established what those deficiencies are, it will not be in a position to verify that an essentially equivalent level of protection is provided in light of safeguards implemented. Therefore, an examination of the law and practices of the third country of destination is crucial to enable a controller to verify whether the law of that third country undermines the effectiveness of the protection afforded by those safeguards. Only following an assessment of the law of the third country is it possible for the controller or processor to determine whether, having regard to appropriate safeguards and supplementary measures, the transfer can operate based on a level of protection essentially equivalent to that which is guaranteed within the European Union. Therefore, while transfers under Article 46 GDPR can occur where the third country does not provide an essentially equivalent level of protection, such transfers

[93] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 125.
[94] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 126.
[95] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 126.
[96] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraphs 132–133.

can only occur where appropriate safeguards are provided by other means. In order for a controller or processor to assess whether appropriate safeguards are provided, it is crucial for the controller or processor to first assess the law and practices of the third country in the context of the transfers, in particular, in respect of access by public authorities.

257. Having assessed the law of the third country, in order to verify and guarantee an essentially equivalent level of protection, the controller or processor must assess whether the appropriate safeguards, enforceable rights and effective legal remedies ensure that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the European Union. This requires an assessment of the appropriate safeguards and supplementary measures in light of the proposed transfers and the law of the third country.

258. The Schrems II judgment is clear that the proposed transfer can proceed only if the controller or processor's assessment has first verified and guaranteed an essentially equivalent level of protection. If the controller or processor has failed to verify and guarantee an essentially equivalent level of protection, it is required to suspend or end the transfer. A controller or processor cannot avoid this obligation to suspend or end a transfer by failing to assess, or failing to fully assess, the relevant law of the third country and the level of protection in light of the appropriate safeguards and supplementary measures. Rather, this full assessment is mandatory before any transfer based on Article 46. Therefore, a failure to verify and guarantee an adequate level of protection renders any subsequent transfers unlawful.

259. In addition to verifying and guaranteeing an essentially equivalent level of protection for the transferred personal data, the controller or processor must also be able to demonstrate that the transfers are provided an essentially equivalent level of protection in accordance with its accountability obligations[97] and its obligations pursuant to Chapter V of the GDPR. This requires, in practice, that a controller or processor must be able to demonstrate that it has verified and guaranteed an essentially equivalent level of protection for the transferred personal data, and it must be able to demonstrate the basis for its conclusion that the standard of essential equivalence is met.

260. Accordingly, the controller or processor must perform and document an assessment of the lawfulness of its transfers that demonstrates that the transfers are provided an essentially equivalent level of protection, and the controller or processor must make such documentation available to the competent supervisory authority upon request. If the controller or processor cannot demonstrate an essentially equivalent level of protection, it must not start, or continue, the transfers.[98] Therefore, a documented data transfer assessment is crucial to a data controller or processor's consideration of proposed transfers before they occur, and to demonstrating that it has verified and guaranteed an essentially equivalent level of protection on an ongoing basis after the transfers commence.

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.[99] The Schrems II judgment

[97] Articles 5(2) and 24 GDPR.
[98] See paragraph 57 of the European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021).
[99] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 107.

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.

262. Relevant guidance from the EDPB on the manner in which controllers such as TikTok Ireland should undertake the task of assessing transfers of personal data to third countries and identifying appropriate supplementary measures is contained in the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021) ('**the Supplementary Measures Recommendations**').[100]

263. Also relevant to the analysis of whether surveillance measures allowing access to personal data by public authorities in a third country comply with Chapter V GDPR and Articles 7, 8 and 52 of the Charter are the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020) ('**the Essential Guarantees Recommendations**').[101]

b) TikTok Ireland's submissions on the legal framework

264. TikTok Ireland's submissions to the Inquiry dispute the nature of the obligation to verify, guarantee and demonstrate that the transferred personal data are afforded a level of protection essentially equivalent to that guaranteed within the European Union. TikTok Ireland disputes that a failure on the part of a controller or processor to comply with this obligation renders subsequent transfers, based on an inadequate assessment, unlawful. In its submissions in response to the Preliminary Draft Decision, TikTok Ireland submitted that, in the event that a controller fails to verify adequately that the requirements of Article 46 are complied with before transferring personal data to a third country, then the competent supervisory authority must carry out this assessment. According to TikTok Ireland, the Schrems II judgment mandates that the DPC must conclude that it is impossible to comply with the SCCs before the DPC can make a suspension order in respect of the transfers.

265. The DPC does not accept TikTok Ireland's submissions regarding the obligation to verify, guarantee and demonstrate an essentially equivalent level of protection. Article 46(1) GDPR places the obligation on the controller or processor to provide appropriate safeguards in respect of a transfer of personal data. The CJEU confirmed in the Schrems II judgment that this requires that the appropriate guarantees must be capable of ensuring a level of protection essentially equivalent for data subjects to that which is guaranteed in the European Union. The Schrems II judgment is unequivocal that it is the responsibility of the controller or processor to verify whether the law of the third country of destination ensures adequate protection having regard to safeguards implemented. The CJEU also outlined that the controller or processor must guarantee such protection. The CJEU was also unequivocal that, where a controller or processor is unable to do so, it must suspend or end the transfers.

266. The obligation on controllers or processors to verify and guarantee that transfers made under Article 46 GDPR are subject to a level of protection essentially equivalent to that which is guaranteed in the European Union is crucial to upholding the fundamental rights of data subjects. Transfers made under Article 46 GDPR do not have the benefit of an adequacy decision adopted by the European Commission concluding that the third

[100] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021).
[101] European Data Protection Board (EDPB), Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020).

country's relevant legislation ensures an adequate level of protection, and are not subject to prior approval by data protection authorities. Indeed, the purpose of Article 46 is to allow transfers to third countries in respect of which the European Commission has not adopted an adequacy decision on the basis that any inadequacies in the protection afforded in the legal order of that third country is compensated for by additional safeguards and supplementary measures. Therefore, as acknowledged by the CJEU in the Schrems II judgment, there is a responsibility on the controller or processor to verify and guarantee that the personal data transferred is subject to a level of protection essentially equivalent to that which is guaranteed in the European Union.

267. Article 46 GDPR must be read in light of Article 44 GDPR, which requires that all provisions of Chapter V of the GDPR must be applied to ensure that the level of protection guaranteed by the GDPR is not undermined. The responsibility on the controller or processor to verify and guarantee an essentially equivalent level of protection to that provided in the European Union applies in the context of the risk that the protection afforded within the European Union can be undermined when personal data moves across borders outside the European Union. When personal data moves across borders, there is a particular risk that the level of protection can be undermined in circumstances where the standards are not enforceable in that third country and, as acknowledged by Recital 116 GDPR, *"supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders"*. As transfers made pursuant to Article 46 GDPR are not subject to adequacy decisions adopted by the European Commission, and are not subject to prior approval by data protection authorities, in order to ensure that the required level of protection is not undermined, it is essential that the controller or processor first verify and guarantee an essentially equivalent level of protection. This is how Article 46 GDPR ensures that the high level of that protection provided within the European Union continues where personal data is transferred to a third country. This standard is necessitated by Article 46 GDPR read in light of Article 44 GDPR.

268. Article 46 GDPR must also be read in light of the accountability obligations in Articles 5(2) and 24 GDPR. Article 5(2) GDPR requires that a controller shall be responsible for, and able to demonstrate compliance with the data protection principles. Article 24 GDPR requires a controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. TikTok Ireland submitted that Articles 5(2) and 24 are not applicable in this manner.[102] It submitted that Article 5(2) GDPR has no application because that obligation applies only to the principles articulated in Article 5(1) GDPR. In this regard, TikTok Ireland submitted that the lawfulness principle provided for in Article 5(1)(a) GDPR refers to the requirement that a controller have a lawful basis for processing under Article 6(1) GDPR. TikTok Ireland reiterated this position in its submissions dated 11 April 2025 on the CSA views. However, it is well-established that when interpreting a provision of EU law, it is relevant take into account not only the wording of the provision concerned, but also its context and the general scheme of the

[102] TikTok Ireland also submitted that these articles are not within the scope of the inquiry. The DPC does not accept this submission. The Commencement Notice clearly expressed issue 2 as concerning whether TikTok can demonstrate that it has fulfilled its Chapter V obligations. The Commencement Notice also expressly reserved the DPC's right to include compliance with additional provisions of the GPDR in connection with the identified issues and to include one or more determinations as to TikTok's compliance with Articles 5(2) and 31 of the GDPR. Furthermore, irrespective of the question of scope, as set out above, it is clear that an interpretation of Article 46 GDPR must take into account not only the wording of the provision concerned, but also its context and the general scheme of the rules of which it forms part and the objectives pursued thereby.

rules of which it forms part and the objectives pursued thereby.[103] Therefore, a controller or processor's accountability obligations are relevant to the obligation on controllers and processors to verify and guarantee an essentially equivalent level of protection. Controllers and processors must have regard to the accountability obligations when performing an assessment of the lawfulness of transfers under Articles 44 and 46 GDPR, having regard also to the considerations set out in recital 74 GDPR. An interpretation of the requirement to perform an assessment under Articles 44 and 46 that takes appropriate account of Articles 5(2) and 24 GDPR is also consistent with the emphasis in Schrems II on the responsibility of a controller to verify whether the law of the third country to which personal data of EEA users is transferred ensures an essentially equivalent level of protection, and to demonstrate this to a supervisory authority exercising its power to review the compliance of such transfers with the GDPR. The CJEU judgment in UZ v Bundesrepublik Deutschland[104] affirmed that that the lawfulness principle provided for in Article 5(1)(a) GDPR refers to the requirement that a controller have a lawful basis for processing under Article 6(1) GDPR. However, the accountability obligations under the GDPR flow not only from Article 5(2), which is applicable in respect of the principles in Article 5(1) GDPR, but also from Article 24, which is applicable to the GDPR generally. Furthermore, it is recalled that data transfers to third countries are a form of data processing in themselves[105] and to ensure the effective application of the level of protection required by Chapter V of the GDPR, it is crucial that the controller or processor is able to demonstrate that level of protection in practice in respect of the relevant transfers.

269. TikTok Ireland submitted that, in the event that a controller fails to verify adequately that the requirements of Article 46 are complied with before transferring personal data to a third country, then the competent supervisory authority must carry out this assessment. TikTok Ireland submitted that Article 24 GDPR does not absolve a supervisory authority *"of its obligations to investigate and assess the adequacy of the protections provided in respect of data transfers made under Article 46 GDPR, as articulated in Schrems II"*.[106]

270. TikTok Ireland's submission in this regard is misconceived for a number of reasons. The purposes of this Inquiry include assessing the lawfulness of TikTok Ireland's transfers of personal data to China. In order for TikTok Ireland to rely on Article 46 for the Data Transfers, TikTok Ireland was obliged to first verify and guarantee an essentially equivalent level of protection. A failure on TikTok Ireland's part to do so would mandate that TikTok Ireland, or failing that, the DPC, suspend or end the transfers. In addition to verifying and guaranteeing an adequate level of protection, TikTok Ireland was also obliged to demonstrate that level of protection, further to its obligations under Article 46 GDPR, having regard to the obligations under Articles 5(2) and 24 GDPR, as set out above.

271. By enforcing this obligation on TikTok Ireland, the DPC is not absolving itself of its duties to investigate the lawfulness of the transfers. To the contrary, the DPC has conducted a detailed inquiry into the lawfulness of the transfers. The DPC has provided multiple opportunities for TikTok Ireland to demonstrate that it has verified and guaranteed that the personal data transferred are afforded a level of protection essentially equivalent to that guaranteed within the European Union. This includes a careful consideration by the DPC of the information submitted by TikTok Ireland in response to the commencement of the Inquiry, subsequent

[103] Case C-395/18, Tim SpA - Direzione e coordinamento Vivendi SA v Consip SpA and Ministero dell'Economia e delle Finanze, judgment of 30 January 2020 (ECLI:EU:C:2020:58).
[104] Case C-60/22, UZ v Bundesrepublik Deutschland, judgment of 4 May 2023 (ECLI:EU:C:2023:373).
[105] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 83.
[106] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 91.

information submitted by TikTok Ireland further to the DPC's requests for further information, information submitted by TikTok Ireland in response to the Statement of Issues, TikTok Ireland's later submissions relating to the 2021 SCCs, TikTok Ireland's submissions in response to the preliminary findings set out in the Preliminary Draft Decision, and TikTok Ireland's subsequent submissions repeatedly made following the Preliminary Draft Decision.

272. The Schrems II judgment is clear that where a controller or processor cannot guarantee the essentially equivalent protection, that controller or processor is required to suspend or end the transfer. Throughout the inquiry, the DPC has carefully assessed whether TikTok Ireland has met its obligations in this regard. The DPC does not accept TikTok Ireland's interpretation that, in the event that a controller fails to verify and guarantee an essentially equivalent level of protection, then the competent supervisory authority must itself seek to verify or guarantee that level of protection. This interpretation is clearly contrary to the scheme of Article 46 GDPR when read in light of Articles 44, 5(2), and 24 GDPR.

c) TikTok Ireland's assessment of the law and practices in China regarding the level of protection of personal data of EEA users the subject of the Data Transfers

273. In order to verify and guarantee that the personal data transferred will be subject to an essentially equivalent level of protection in conjunction with appropriate safeguards and supplementary measures, it is crucial that the controller or processor first assesses the law and practices of the third country in the context of the transfers. A comprehensive assessment of the law and practices of the third country as they relate to the transfers is required in order to verify whether appropriate safeguards and supplementary measures are capable of providing an essentially equivalent level of protection. This assessment is also crucial to identifying which safeguards and measures are necessary to achieve an essentially equivalent level of protection. Therefore, the DPC will now consider TikTok Ireland's assessment of the law and practices in China as they relate to the Data Transfers.

274. During the Inquiry, TikTok Ireland provided the DPC with copies of the following Data Transfer Assessments relating to transfers to the China Group Entities:

(i) Data Transfer Assessment dated 12 October 2021 relating to transfers under the 2010 SCCs,

(ii) Data Transfer Assessment dated 13 October 2022 relating to transfers under the 2010 SCCs,

(iii) Data Transfer Assessment dated 19 December 2022 relating to transfers under the 2021 SCCs.

(iv) Data Transfer Assessment dated "October 2023" relating to transfers under the 2021 SCCs.

(v) Data Transfer Assessment dated "July 2024" relating to transfers under the 2021 SCCs.

275. As set out above, the temporal scope of this inquiry concerns transfers taking place from 29 July 2020 to 17 May 2023. The Data Transfer Assessments dated 12 October 2021, 13 October 2022 and 19 December 2022 are relevant to that temporal scope. Some updates made by TikTok Ireland to the October 2023 and July 2024 Assessments are relevant to considering the state of play regarding Chinese law during the temporal scope of the Inquiry. For example, TikTok Ireland's October 2023 Data Transfer Assessment was created after the DPC's Preliminary Draft Decision and included additional analysis regarding the legal jurisdiction of Chinese authorities to compel disclosure of remotely accessible EEA User Data. That additional analysis applies equally to questions of Chinese law during the temporal scope of the inquiry. In particular, this analysis is relevant to

the position put forward in the 12 October 2021[107], 13 October 2022[108], and 19 December 2022[109] Assessments that, due to the territorial scope of jurisdiction of Chinese law, Chinese authorities do not have legal jurisdiction to compel organisations and individuals to provide data that are not domestically stored within the territory of China. Therefore, the DPC has considered this additional information for the purposes of this Decision in order to ensure that TikTok Ireland has been provided with every opportunity to demonstrate that it verified and guaranteed an essentially equivalent level of protection in respect of the Data Transfers. In particular, the DPC notes that this additional information seeks to support positions put forward in the Data Transfer Assessments dated 12 October 2021, 13 October 2022 and 19 December 2022. In addition to the Data Transfer Assessments, TikTok Ireland made extensive and detailed submissions throughout the Inquiry regarding the application of Chapter V of the GDPR to its Data Transfer Assessments. The DPC has carefully considered those submissions for the purposes of this Decision.

276. The Data Transfer Assessments are each stated to have been completed in accordance with TikTok Ireland's EEA Data Transfer Policy.[110] The policy objective of TikTok Ireland's EEA Data Transfer Policy is stated as:

> Having regard to Art. 24 of the General Data Protection Regulation ("GDPR"), the objective of this Policy is to provide a framework for ensuring that TikTok's Data Transfers are undertaken in a manner that is consistent with TikTok's obligations under EU law, the GDPR, relevant case-law, and with relevant regulatory guidance.[111]

277. The Data Transfer Assessments are divided as follows:

(i) Section 1 – Summary of the transfers and transfer mechanism,

(ii) Section 2 – Assessment of the effectiveness of the transfer mechanism,

(iii) Section 3 – Supplementary measures to safeguard data.

278. Section 2 of each Data Transfer Assessment sets out TikTok Ireland's assessment of whether the law or practices in force in China could potentially undermine the effectiveness of the contractual safeguards contained in the SCCs relied on under Article 46(2)(c) GDPR. TikTok Ireland indicated that the assessment in Section 2 of the Data Transfer Assessment had been made having regard to the Essential Guarantees Recommendations.

279. TikTok Ireland outlined that that the legal analysis in Section 2 of each Data Transfer Assessment has been *"prepared by one of China's leading independent law firms"*. The law firm identified is Fangda Partners. In this connection, TikTok Ireland states that *"Fangda Partners' data protection and technology practice is ranked Band 1 / Tier 1 by leading global legal directories, including Chambers & Partners and The Legal 500."*[112]

280. In this part of the Decision, the DPC will consider TikTok Ireland's assessment under the following headings:

---

[107] At page 14.
[108] At page 19.
[109] At page 25.
[110] TikTok Ireland's Response dated 12 October 2021, Schedule A, Document 6.
[111] EEA Data Transfer Policy, adopted 15 March 2021, at page 1.
[112] Data Transfer Assessment – China Group Entities dated 12 October 2021, at page 1, Data Transfer Assessment – China Group Entities dated 13 October 2022, p. 1, Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 2.

(i) Regulation of data privacy,

(ii) Regulation of public authority access to personal data,

(iii) Regulatory supervision,

(iv) Right of redress,

(v) International treaties.

i. Preliminary matter regarding the assessment of Chinese law

281. Before assessing TikTok Ireland's compliance with its obligation to assess the law and practices in effect in China, at the outset, it is relevant to state that, the DPC in this Decision does not engage in a legal interpretation of Chinese law, which is an exercise reserved for experts in Chinese law. The normal rule in Irish law is that the law of a foreign jurisdiction is treated as a matter of fact, and in general would be established by the independent expert evidence of a suitably qualified lawyer with knowledge of and expertise in the law of that foreign jurisdiction.[113] It is considered by the courts, applying the rules of evidence that apply in legal proceedings, to be unsafe to try to determine questions of the content or interpretation of foreign law by looking at the statutory provisions or case law from the foreign jurisdiction concerned. Rather, it is desirable that a decision-maker should have *"[…] an appropriate level of assurance so that [it] can determine with confidence what the true position in the law of the relevant foreign jurisdiction actually is."*[114]

282. In the context of the Inquiry, the DPC must ensure that there is sufficient information and evidence to enable the DPC to review TikTok Ireland's assessment, and ultimately to conclude that TikTok Ireland has verified and guaranteed that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within the European Union. As set out above, there is an obligation on TikTok Ireland to demonstrate that it has verified and guaranteed an essentially equivalent level of protection. Therefore, this Decision considers whether TikTok Ireland complied with its obligation to verify and guarantee an adequate level of protection in light of all relevant considerations, and whether it has demonstrated same.

283. The DPC has considered the manner in which it should assess information relating to the content, meaning or effect of Chinese law in the context of this Decision. Regarding the information furnished by TikTok Ireland, in circumstances 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"*, the DPC has taken the information at its height, and at face value, with regard to its veracity. Insofar as additional information submitted by TikTok Ireland after the temporal scope seeks to support positions set out in the Data Transfer Assessments relevant to the temporal scope, including the Second Xu Report, the DPC has had regard to that information at its height for the purposes of this Decision.

284. In the Statement of Issues, the DPC identified the Milieu Report prepared for the EDPB as a potential source of information that may be relevant to TikTok Ireland's assessment of the law and practices in effect in China with respect to the protection of personal data, and invited TikTok Ireland to make submissions in respect of same. The Milieu Report is a legal study of government access to data in third countries, including China, carried out by researchers from the Centre for IT and IP Law of KU Leuven with support from Milieu Consulting

[113] *O'Callaghan v. O'Sullivan* [1925] 1 I.R. 90 at p. 112, *O'Brien v. Clerk of Dáil Eireann* [2016] IEHC 597, [2016] 3 I.R. 384 at p. 397, *Walsh v. National Irish Bank Limited* [2013] IESC 2, [2013] 1 I.R. 294, pp. 339–340.
[114] *Walsh v. National Irish Bank Limited* [2013] IESC 2, [2013] 1 I.R. 294, p. 350.

SRL. As noted on page 2 of the Milieu Report, the EDPB does not guarantee the accuracy of the data included in the study, and the study does not reflect the official opinion of the EDPB.

285. Nonetheless, insofar as the study presented an analysis relating to the legal framework for protection of personal data in China from the standpoint of the requirements of the GDPR for transfers of personal data to third countries, the DPC considered it appropriate that TikTok Ireland be invited to comment on it, in particular where the study, prepared for the benefit of the EDPB, was expressed to *"contain an overview of the relevant information in order for the [supervisory authorities] to assess whether and to what extent legislation and practices in the abovementioned countries imply massive and/or indiscriminate access to personal data processed by economic operators"*.

286. As part of its response to the Statement of Issues, TikTok Ireland submitted that the methodology of the study the subject of the Milieu Report had a number of shortcomings, including the question of the level of expertise in Chinese law and practices and other methodological concerns TikTok Ireland had with the report. TikTok Ireland submitted, in light of those matters, that the Milieu Report should not be considered a credible reference point for Chinese law and practice.[115]

287. TikTok Ireland furnished the First Xu Report, the scope of which was to *"to consider whether the Milieu Report, with respect to Chinese law and practice, is inaccurate in any respects and to provide any other observations with respect to the Milieu Report which may be relevant to the Inquiry"*.[116] This expert opinion sets out Professor Ke Xu's analysis of the matters outlined in the Milieu Report, which criticised its methodology.

288. In light of the above, insofar as the Milieu Report presents a different analysis of the law and practices in force in China with respect to the protection of personal data than the assessment made by TikTok Ireland in Section 2.1 of each Data Transfer Assessment, the DPC must evaluate that material, including the weight to be afforded to that material in a manner which reflects the difference in probative weight and value of the opinion or evidence given by an expert.

289. In that regard, the DPC considers that it must attach greater weight to the analysis of the legal framework in China that was put forward by TikTok Ireland than the analysis presented in the Milieu Report.

290. The First Xu Report is expressly framed by way of response to the Milieu Report. TikTok Ireland adduced the First Xu Report in response to the DPC's stated intention to rely upon the Milieu Report. The content of the First Xu Report does not address all matters that TikTok Ireland has considered for the purpose of the Data Transfer Assessments and does not speak to TikTok Ireland's analysis in that regard.

291. TikTok Ireland obtained the Second Xu Report to address concerns expressed in the Preliminary Draft Decision regarding Chinese law. The Second Xu Report also does not address all matters that TikTok Ireland has considered for the purpose of the Data Transfer Assessments, however, it states the view that the statement of Chinese law contained in Section 2 of the December 2022 Data Transfer Assessment is an accurate statement of Chinese law as at December 2022.

292. The Fangda Report, as set out below, states that the statement of Chinese law contained in Section 2 of the December 2022 Data Transfer Assessment is an accurate statement of Chinese law as of December 2022.

[115] TikTok Ireland's Submission dated 15 September 2022, at pages 16 - 17.
[116] The First Xu Report, at page 1.

ii. Overall summary of assessment

293. In each of TikTok Ireland's 2021 and 2022 Data Transfer Assessments (with very minor textual amendments) the overall summary of assessment in respect for transfers under both the 2010 SCCs and the 2021 SCCs under Section 2 was as follows:

> Based on the assessment of China's current legal framework, it provides for: (1) binding applicable data protection laws (although they may not be entirely equivalent to EU standards); (2) rules circumscribing surveillance powers, including requirements for ex ante authorisation; (3) surveillance regimes that are subject to legality and proportionality requirements; (4) administrative oversight; (5) various authorities authorized to enforce the data protection laws, with the Cyberspace Administration of China being tasked to lead and coordinate the enforcement activities among the ministries; and (6) rights of individual redress against abuses of power and unlawful surveillance and in relation to breaches of data protection laws more generally. However, for the reasons explained below, we understand that there are aspects of the current legal framework that preclude a finding of essential equivalence to EU law, even where SCCs are used. In this regard, 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 […].

iii. Regulation of data privacy

294. Section 2.1 of each Data Transfer Assessment sets out TikTok Ireland's assessment of the regulation of data privacy in China.

295. In respect of the regulation of data privacy, TikTok Ireland's 2021 and 2022 Data Transfer Assessments concluded, in respect of both transfers under the 2010 SCCs and under the 2021 SCCs that, while Chinese law and practice offered a high level of safeguards, the level of protection diverged from that required by EU law.

296. TikTok Ireland's assessment in Section 2.1 of each Data Transfer Assessment had regard to, inter alia, the following measures, which, where indicated, TikTok Ireland has also provided to the DPC in unofficial English translation as part of the materials furnished in the Inquiry:

(i) The Constitution of the People's Republic of China ('**the PRC Constitution**')[117]

(ii) The Personal Information Protection Law in effect from 1 November 2021,[118]

(iii) The Data Security Law in effect from 1 September 2021,[119]

(iv) The Cybersecurity Law in effect from 1 June 2017,[120]

(v) The Civil Code in effect from 1 January 2021,[121]

(vi) The Criminal Law in effect from 3 January 2021,[122]

---

[117] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.12.
[118] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.1.
[119] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.2.
[120] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.2.
[121] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.9.
[122] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.8.

(vii) Sector-specific legislation,

(viii) Local and regional bye-laws, and

(ix) The National Standard of Information Security Technology – Personal Information Security Specification.

297. The Data Transfer Assessments in Section 2.1 of each assessment were primarily directed to an assessment of the legal framework in place in China by reference to Guarantee A in the Essential Guarantees Recommendations. However, the DPC notes that Guarantee A concerns, in particular, the assessment of whether the law and practices with regard to surveillance by public authorities in a third country are based on clear, precise and accessible rules, in the manner envisaged by Articles 8(2) and 51(2) of the Charter.[123] Section 2.1 does concern a set of law and practices that are broader in scope than surveillance measures, which are more particularly dealt with in Section 2.2 of the Data Transfer Assessment. Therefore, while Guarantee A is undoubtedly relevant to Section 2.1, the DPC will also consider it in relation to the discussion of Section 2.2 below.

298. Section 2.1 of each Data Transfer Assessment outlined the above laws and guidelines, and in particular, analyses the features of the laws that contain key concepts that are similar to, but not entirely equivalent to, the key concepts present in the GDPR, including, inter alia, concepts such as personal information, sensitive personal information, terminology for parties processing personal information, lawful basis for personal information processing, transparency, data minimisation, purpose limitation, accuracy and retention, and data security, and data subject rights. The Data Transfer Assessments further note that foreign data subjects also enjoy the protection of the relevant laws, and, in particular, various data subject rights under such laws, when their personal information is transferred to or remotely accessed in China, and cites examples of case law where the personal information rights of foreigners were protected before the Chinese courts.[124]

299. TikTok Ireland's overall conclusion in respect of the general legal framework for the regulation of data privacy in China is that generally safeguards for the protection of personal data exist, but are not essentially equivalent to those required in the EU and do diverge from them in some respects. It is relevant to note that the situation in this regard has changed to an extent during the course of the Inquiry, where, prior to the entry into effect of the Personal Information Protection Law on 1 November 2021, TikTok Ireland had identified as a potential issue the fact that there was no single comprehensive data protection law similar to the GDPR for the purpose of offering comprehensive protection of personal data in China.[125] However, TikTok Ireland notes this has since changed, in circumstances where *"[t]he PIPL introduced comprehensive data protection rules and principles applying to both private companies and public authorities and has been applied and implemented in a manner giving rise to an increased level of protection for personal data in China."*[126] Nonetheless, TikTok clearly acknowledged a divergence by the protection afforded by the law of China compared with EU law, even where SCCs are used.

300. TikTok Ireland considers, that in practice, the divergence does not present issues on the basis that its legal analysis is that Chinese authorities are not lawfully entitled to compel organisations and individuals to provide data that are not domestically stored within the territory of China.

---

[123] European Data Protection Board (EDPB), Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020) at pages 8-10.

[124] Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 16, and Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 21–22.

[125] TikTok Ireland's Response dated 12 October 2021, at page 4.

[126] TikTok Ireland's Response dated 20 June 2022, at page 23.

iv. Regulation of public authority access to personal data in China

301. Section 2.2 of each Data Transfer Assessment set out TikTok Ireland's assessment of the regulation of public authority access to personal data in China.

302. In respect of the regulation of public authority access to personal data in China, TikTok Ireland's 2021 and 2022 Data Transfer Assessments concluded that, while Chinese law provides some safeguards, it materially diverges from EU standards.

303. TikTok Ireland's assessment in Section 2.2 of each Data Transfer Assessment had regard to, inter alia, the following surveillance laws, which, where indicated, TikTok Ireland has also provided to the DPC in unofficial English translation as part of the materials furnished in the Inquiry:

(i) The Criminal Law in effect from 3 January 2021,[127]

(ii) The Criminal Procedure Law,[128]

(iii) The National Intelligence Law in effect from 27 April 2018,[129]

(iv) The Counter-Espionage Law,[130]

(v) The Anti-Terrorism Law in effect from 27 April 2018.[131]

(vi) The Cyber-Security Law in effect from 1 June 2017,[132]

(vii) The PRC Data Security Law in effect from 1 September 2021,[133] and

(viii) The Personal Information Protection Law in effect from 1 November 2021.[134]

304. TikTok Ireland also identified as relevant a number of public statements by the Chinese authorities relevant to policy on public authority access to private data,[135] including, inter alia, the Global Data Security Initiative of 8 September 2020.[136] Each of the above measures were analysed in detail in Section 2.2 of the Data Transfer Assessments.

305. The overall conclusion reached by TikTok Ireland in respect of public authority access to personal data is that, while there is circumscription of the surveillance measures provided by Chinese law, the controls on data access by Chinese authorities are not as prescriptive and clear as what is required by the EU standard.

---

[127] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.8.
[128] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.7.
[129] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.4.
[130] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.5.
[131] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.6.
[132] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.3.
[133] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.2.
[134] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 5.1.
[135] Data Transfer Assessment – China Group Entities dated 13 October 2022, at pages 30-31 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 40-41.
[136] TikTok Ireland has provided the hyperlink to the text of this policy on the website of China's Ministry of Foreign Affairs at: <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html>.

306. TikTok Ireland outlined that although principles of legality, necessity, and proportionality are reflected both in legislation and judicial decisions that apply to surveillance measures, and Chinese authorities are required to follow such principles, the more granular criteria for granting approval for public authority access to personal data tend not to be published and application of the measures are not as clear and precise as required by the EU standard.

307. For that reason, TikTok Ireland noted that it is difficult to establish whether the seriousness of the interference entailed by a given surveillance measure is, in practice, balanced against the importance of the public interest objective pursued by the measure in order to comply with the principle of proportionality to the extent required by the EU standard, and that measures are actually applied in practice only in so far as is strictly necessary, such that there is a connection between the data obtained and the objective pursued to the extent required by the EU standard.[137]

308. This is, in effect, an acknowledgement on the part of TikTok Ireland that there is a doubt that Chinese law complies with Guarantees A and B of the Essential Guarantees Recommendations formulated by the EDPB.

309. As outlined above, Guarantee A of the Essential Guarantees Recommendations addresses the need for law and practices regulating the processing of personal data to itself define the scope of the limitation on the exercise of the right concerned and be based on clear, precise and accessible rules and subject to minimum safeguards.

310. Guarantee B of the Essential Guarantees Recommendations is directed to whether such law and practices respect the principles of necessity and proportionality as developed in the CJEU's case law, including that:[138]

(i) legislation interfering with the rights to privacy and to data protection must be assessed by measuring the seriousness of the interference entailed by the limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness,

(ii) such legislation must be based on clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, must be legally binding under domestic law, and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary,

(iii) it must always meet objective criteria that establish a connection between the data to be retained and the objective pursued.

311. TikTok Ireland stated in Section 2.2 of the Data Transfer Assessments that there are Chinese laws that materially diverge from EU standards (any such laws are referred to collectively as '**the Problematic Laws**' for the purposes of this Decision). As set out in further detail below in this Decision, TikTok Ireland does not

[137] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 14-15, Data Transfer Assessment – China Group Entities dated 13 October 2022, at pages 20-21 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 26-27.

[138] European Data Protection Board (EDPB), Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020) at pages 10-12 and see also the Judgment of the CJEU of 6 October 2020, *La Quadrature du Net*, C-511/18, EU:C:2020:791, paragraphs 131–133.

consider that the material divergences in the Problematic Laws undermine the effectiveness of the SCCs because *"Chinese authorities are not lawfully entitled to compel organisations and individuals to provide data that are not domestically stored within the territory of China".*[139] TikTok Ireland considers therefore that the Problematic Laws cannot be applied to compel the China Group Entities, or individuals in China working for them, to disclose the remotely accessible EEA User Data. The Problematic Laws as outlined at Section 2.2 of the Data Transfer Assessments include, inter alia:

> "[…] The National Intelligence Law provides that any organisation or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law. The scope of the terms "organisation and/or citizen", as well as the terms "support, assist and cooperate" are not clearly defined but, properly construed based upon the principle of "law-based administration", does not appear to require organisations to provide personal information as part of such support, assistance or co-operation. This is further supported by the fact they are to be defined "in accordance with the law", "respecting and safeguarding any individuals' human rights and legitimate rights and interests of individuals and organisations" (Article 8 of National Intelligence Law); "not infringing upon the legitimate rights and interests of any citizens and organisations" (Article 19 of National Intelligence Law), etc.
>
> […] The Counter-Espionage Law […] requires organisations to "facilitate and provide other assistance" in counter-espionage efforts – this term is not clearly defined and different interpretations could be taken in practice, but, properly construed based upon the principle of "law-based administration", does not appear to require organisations to provide personal information. These surveillance activities can only be carried out for the needs of counterespionage work (the scope of which is defined in Article 38 of the Counter-Espionage Law) and shall only be targeted at the 'relevant' organisations and individuals. The national security authorities are also required to abide by statutory procedures (including for example ex-ante authorisation) before and while conducting counter-espionage related surveillance activities and to conduct it 'in accordance with law, respect and protect human rights, and protect citizens' and organisations' lawful rights and interests'.
>
> "[…] Article 18 of the Anti-Terrorism Law requires that "telecommunication business operators and internet service providers shall provide technical interfaces, decryption and other technical support and assistance for public security authorities and state security authorities to prevent and investigate terrorist activities in accordance with the law". This requirement may give rise to concerns that data processed by entities in China may not be subject to safeguards equivalent to EU standards, even if such data would be encrypted by the telecommunication business operator or internet service provider. However, the Anti-Terrorism Law does not contemplate an extra-territorial effect – save for one exception provided in Article 11 of the Anti-Terrorism Law which contemplates extraterritorial effect under the PRC Criminal Law where any terrorist activities outside China are against the state or citizens of China.
>
> […] The PRC Cybersecurity Law also imposes obligations on network operators to provide "technical support and assistance" to the public security bureau and the national security bureau for national

[139] Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 27.

security or criminal investigation needs in accordance with law. This term is not clearly defined and different interpretations could be taken in practice, but, properly construed based upon the principle of "law-based administration", it does not appear to require organisations to provide personal information."[140]

312. TikTok Ireland acknowledged that, while there are some safeguards, they materially diverge from the EU standard. However, it considers that in practice, the divergence does not present issues on the basis that its legal analysis is that Chinese authorities are not lawfully entitled to compel organisations and individuals to provide data that are not domestically stored within the territory of China.

v. Regulatory supervision

313. Section 2.3 of each Data Transfer Assessment sets out TikTok Ireland's assessment of regulatory supervision of laws protecting the right to protection of personal information in China, including, in particular, public authority access to personal information.

314. The issue arising relates to Guarantee C in the Essential Guarantees Regulations which envisages that interferences with the right to privacy and protection of personal data should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body.[141]

315. In respect of the regulation of regulatory supervision, TikTok Ireland's 2021 and 2022 Data Transfer Assessments concluded that, while Chinese law provides some safeguards, it materially diverges from EU standards.

316. The main factors considered in the assessments under Section 2.3 include:

(i) the compliance of Chinese authorities' access to privately-held data is subject to the internal oversight mechanism of the Chinese authorities and the respective organisations' superior authorities, e.g. ex-ante approval, procedural requirements, examination review, and disciplinary sanctions, and

(ii) the enforcement of Chinese data protection laws by the Cyberspace Administration of China (the primary data protection authority in China), and regulatory authorities such as the Ministry of Public Security, the Ministry of Industry and Information Technology, the State Administration for Market Regulation, the Ministry of Science and Technology, The People's Bank of China, and the China Banking and Insurance Regulatory Commission, the People's Procuratorates, and the National Supervisory Commission,

(iii) judicial oversight of the in the case of litigation by an individual or the People's Procuratorates.

317. TikTok Ireland highlighted a number of examples of enforcement by the different regulatory authorities outlined above.

318. TikTok Ireland further clarified that the Cyberspace Administration of China and sectoral regulators do not have oversight of national security agencies from a data protection perspective, but submits that the lack of

[140] See Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 35-39.
[141] European Data Protection Board (EDPB), Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020) at pages 12–13.

oversight of national security agencies from a data protection perspective is similar to the position in the EU, given the carve out for national security activities in the GDPR. This refers to:

(i) Recital 16 GDPR, which provides that: *"[t]his Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union*,"

(ii) Article 2(2)(a) which provides that the GDPR does not apply to processing of personal data in the course of an activity which falls outside the scope of Union law,

(iii) Article 23(1)(a) GDPR, which provides for data subject rights to be restricted where such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard national security.

319. However, the relevance of this submission is limited, where in Schrems II, the CJEU made clear that the assessment of a transfer under Article 46 GDPR corresponds to the matters set out, in a non-exhaustive manner, in respect of the law of the third country concerned, in Article 45(2) GDPR, including, under Article 45(2)(a) *"relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data"*.[142]

320. TikTok Ireland considers that there is, in any event, some independent oversight of national security agencies in China with respect to surveillance, as review of surveillance measures can occur by way of internal oversight (i.e. pre-approval of surveillance measures), judicial oversight, and by way of the National Supervisory Commission and People's Protectorates.[143]

321. TikTok Ireland's overall assessment under Section 2.3 has changed over time. In the Data Transfer Assessment dated 12 October 2021, and in its Response dated 15 September 2022 considering the situation under the 2010 SCCs, it considered that the regulatory supervision in China afforded a high level of safeguards, but diverged from the EU standards. In the Data Transfer Assessment dated 13 October 2022, however, still considering the position under the 2010 SCCs, it considered that regulatory supervision in China contained some safeguards, but materially diverged from EU standards. The same assessment of material divergence from EU standards was made in the Data Transfer Assessment dated 19 December 2022, considering the position under the 2021 SCCs.

322. TikTok Ireland's general assessment in the Data Transfer Assessments is that, while the Chinese laws set out in Section 2.2. of each Data Transfer Assessment contain various requirements for prior approval before a Chinese public authority can obtain data in accordance with the powers granted under those laws:

> there is no mechanism for prior review and approval by a judge or other independent body outside the Chinese authority (e.g. administrative body or parliamentary body) whose decision is binding and

[142] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 104.
[143] Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 35 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 45.

is as independent of government as required by [the EU standard/European Essential Guarantee C], the rules and criteria for internal approval tend not to be published and regulatory authorities may not be as independent of government as certain regulatory authorities in the EU."[144]

323. Consequently, its view is that regulatory supervision in China materially diverges from EU standards.

324. TikTok Ireland also stated, in respect of the independence of the Cyberspace Administration of China and the various regulatory authorities that may enforce the Personal Information Protection Law, the Data Security Law, and the Cybersecurity Law, that:

> Regulatory authorities operate as part of the Chinese government. As explained at page 19 of the Data Transfer Assessment, the CAC coordinates with the Ministries of the Chinese government on the legislation and application of law related to personal information protection and cyber security. Further, the regulatory authorities responsible for supervising and administering data protection matters of private companies under the PIPL are Ministries of the Chinese government and local branches. In contrast, under Article 8(3) of the EU's Charter of Fundamental Rights, EU data protection agencies operate independently.
>
> As a result, it could be observed that Chinese regulatory authorities are not as independent of the government as certain authorities in the EU. However, the regulatory authorities are independently supervised. The [National Security Commission] which is responsible for supervising the administrative authorities performing their powers, is independent from the Ministries of the Chinese Government and is accountable to the National People's Congress and the Standing Committee of the National People's Congress which represents the highest state power in China.[145]

325. TikTok Ireland considers, nonetheless, that in practice, the divergence from the EU standard with regard to regulatory supervision does not present issues on the basis of its legal analysis that the Chinese authorities do not have legal jurisdiction to compel organisations and individuals to provide data that are stored outside of the territory of China.

vi. Rights of redress

326. This element of the assessment is viewed through the prism of Guarantee D in the Essential Guarantees Recommendations, which asks whether, under the law and practices in effect in a third country, in particular those relating to surveillance by public authorities, the rights of data subjects under Article 47 of the Charter to an effective remedy before a tribunal are protected.[146]

---

[144] Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 34; Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 44; Data Transfer Assessment – China Group Entities dated October 2023, at page 78.
[145] TikTok Ireland's Response dated 20 June 2022, at page 41.
[146] European Data Protection Board (EDPB), Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020) at pages 13–14.

327. Section 2.4 of each Data Transfer Assessment sets out various rights of redress that individuals, including foreign individuals, may exercise in respect of breach of privacy and unlawful processing of personal information, including, as summarised by TikTok Ireland:[147]

(i) the right under the National Intelligence Law, Counter-Espionage Law and Anti-Terrorism Law to submit a complaint or report against a Chinese authority that goes beyond its authority, abuses its power or otherwise violates applicable laws,

(ii) the right to apply for administrative review of a relevant measure, which results in escalation to a higher level of government agency,

(iii) the right to complain to the National Supervision Commission,

(iv) the right to complain or report to governmental authorities performing personal data protection duties,

(v) the right under the Criminal Procedure Law to file a petition or complaint to a judicial authority that apply the measures or, where a Chinese authority is acting in its capacity as a government agency, other rights such as the right to sue the authority,

(vi) the right under the Criminal Procedure Law and the Rules of Criminal Procedure for People's Procuratorates to submit a report to the competent People's Procuratorates if they consider any technical investigative measures (e.g. surveillance) have been applied to them illegally, coupled with the right to appeal to the superior People's Procuratorate if not satisfied with the handling of the complaints by the People's Procuratorate,

(vii) the right to bring an administrative law suit, and

(viii) the right to bring a civil lawsuit against a private company for breach of their right to privacy or personal information protection, including (a) the right to seek compensation for infringement of the Personal Information Protection Law or seek specific performance of a right under the Personal Information Protection Law; (b) tort claims for infringing the right to privacy; and (c) civil claims under the Civil Code for breach of the right to privacy.

328. In respect of the regulation of rights of redress, TikTok Ireland's 2021 and 2022 Data Transfer Assessments concluded that, while Chinese law provides a high level of safeguards, it diverges from EU standards.

329. The shortcomings TikTok Ireland identifies in respect of the remedies available to EEA Users in China relate to the possibility that persons the subject of investigations or surveillance by a public authority may not be informed that their personal information is or was being processed, in particular in that:[148]

(i) Chinese authorities are permitted by law to impose confidentiality obligations in the process of investigation or law enforcement and there is no specific obligation under Chinese law to inform a data subject once surveillance is over. As a result, a person may not be informed that a Chinese authority has obtained their data in certain cases. This could impact on their ability to exercise their rights, including their rights of redress (although if an investigation resulted in a prosecution, for

[147] Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 42 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 53.
[148] Data Transfer Assessment – China Group Entities dated 13 October 2022, at pages 42-43 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 54-55.

example, under the Anti-Terrorism Law or the Counter-Espionage Law, the information would be disclosed to the person concerned as part of the case file),

(ii) the Personal Information Protection Law separately requires public bodies to inform the individuals about the proposed access to and processing of their personal information for performing their statutory duties, except where they are subject to confidentiality obligations provided by laws or where giving notice would impede the performance of their duties. Although this could result in Chinese authorities notifying individuals upon the authority obtaining their data or at a later point when satisfied doing so will not impinge upon an investigation. However, there is, as of yet, no evidence that this has become a practice following the introduction of the Personal Information Protection Law,

(iii) arising from the above, it remains possible that in at least certain cases an individual may not be informed that their data has been obtained by a Chinese public authority. Consequently, whilst Chinese law provides a high level of safeguards regarding the right of redress, TikTok Ireland considers that it diverges in this respect from what is required by the EU standard.

330. TikTok Ireland outlined 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, including, for example, where the subject matter of the request concerns a state secret, national intelligence, or co-operation with criminal investigative measures imposed by a public authority.[149]

331. TikTok Ireland has also, in its Response dated 20 June 2022, and reiterated in its Submission dated 15 September 2022, made the points that:

(i) Recital 108 GDPR provides that safeguards under Article 46 GDPR can take into account the availability of enforceable data subject rights and effective legal remedies *"[…] in the Union or in a third country."*

(ii) It is clear from this that the enforceable data subject rights and effective legal remedies required under Article 46(1) GDPR can be in either the Union or a third country, and need not be available in both. In other words, they need not be in the destination country. This was acknowledged by the CJEU in *Schrems II.*

(iii) EEA users have rights that are enforceable in Ireland against TikTok Ireland and the China Group Entities.

(iv) In particular, data subjects had enforceable rights and effective remedies against TikTok, under both the GDPR and the 2010 SCCs, and against China Group Entities under the 2010 SCCs. The 2010 SCCs were governed by Irish law, and data subjects could refer matters in this regard to, as applicable, the Irish courts, mediation, an independent person or the DPC under clause 7 of the 2010 SCCs. They could also complain to the DPC with respect to the processing of their personal data and TikTok, as

[149] Data Transfer Assessment dated 12 October 2022, at page 16, TikTok Ireland's Response dated 20 June 2022, at pages 11-13, Data Transfer Assessment dated 13 October 2022, at page 44, Data Transfer Assessment dated 19 December 2022, at page 55.

controller, was accountable under the GDPR for the processing by it and its processors. This satisfied the requirement under Article 46(1) GDPR.

332. TikTok Ireland also submitted that EEA users now have increased enforceable rights and effective legal remedies as third party beneficiaries pursuant to the 2021 SCCs, which facilitate effective individual redress and ensure effective enforcement.[150] In this regard, TikTok Ireland has submitted that, whilst they are not supplementary measures, the 2021 SCCs provide data subjects with a suite of enforceable rights and remedies as third-party beneficiaries under the 2021 SCCs:[151]

(i) EEA users have the right to obtain a copy of the SCCs under Clause 11(a) of the 2021 SCC.

(ii) They have to be informed of requests by public authorities under Clause 15(1)(a) of the 2021 SCCs.

(iii) EEA users have the right to have complaints dealt with and disputes resolved promptly under Clause 11(a) and (b) of the 2021 SCCs.

(iv) EEA users have the right to invoke third party beneficiary rights under the 2021 SCCs against the China Group Entities and lodge a complaint with the DPC or the supervisory authority of their habitual residence under Clause 11(c)(i) of the 2021 SCCs. The China Group Entities submit themselves to the jurisdiction of the DPC under Clause 13(b) of the 2021 SCCs, and, similarly to Article 31 GDPR, agree to cooperate with the DPC in any procedures aimed at ensuring compliance with the 2021 SCCs. They also agree, under Clause 11(e) of the SCCs, to abide by a decision that is binding under the applicable EU or Member State law (and, as companies belonging to the same corporate group as TikTok, there is no concern that a China Group Entity would not do so as a matter of practice).

(v) If an EEA user invokes a third-party beneficiary right under the 2021 SCCs against a China Group Entity, he/she may refer the dispute to the courts of the Member State in which they have their habitual residence or to the Irish courts under Clause 11(c)(ii) of the 2021 SCC and under Clause 18 of the 2021 SCCs, legal proceedings can be brought in Ireland against both TikTok and the China Group Entities to enforce their rights and remedies under the 2021 SCCs. Under Clause 11(d) of the 2021 SCCs the China Group Entities also accept that an EEA User may be represented by a non-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

(vi) Under Clause 12(b) of the 2021 SCCs, the China Group Entities are liable to EEA Users, and EEA Users are entitled to receive compensation, for any material or non-material damages that they cause an EEA User by breaching the third-party beneficiary rights under the 2021 SCCs,

(vii) Under Clause 12(c) of the 2021 SCCs, EEA users have a right to compensation against TikTok, including for breaches by China Group Entities.

(viii) Under Clause 12(d) of the 2021 SCCs, where TikTok and a China Group Entity is responsible for any damage caused to an EEA User as a result of a breach of the 2021 SCCs, they are jointly and severally liable and the EEA User is entitled to bring an action in court against any of them.

[150] TikTok Ireland's Submission dated 19 December 2022, at page 3.
[151] TikTok Ireland's Submission dated 19 December 2022, at pages 19-22.

333. The DPC accepts TikTok Ireland's submission that, in light of recital 108 GDPR, enforceable data subject rights and effective legal remedies for the purpose of Article 46 GDPR may be provided for in the Union or in a third country.[152] However, it is relevant equally to note the CJEU's observation in Schrems II that:

> The existence of […] effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.[153]

334. For similar reasons, the DPC considers that the existence or absence of independent regulatory supervision in China is of particular importance in the present context in addition to those remedies which may be available to EEA users in the EU. The existence of robust independent regulatory supervision in a third country is especially important where a public authority has powers to obtain personal data and to impose confidentiality obligations on the person or entity receiving the request to prevent the data subject being informed of such access. TikTok Ireland has acknowledged that, although it considers this risk to be remote, it is nonetheless a risk which exists in the context of the Chinese legal framework, which gives rise to a divergence with EU law.

335. Again, TikTok Ireland considers, that in practice, the divergence does not present issues on the basis that its legal analysis is that the Chinese authorities do not have legal jurisdiction to compel organisations and individuals to provide data that are stored outside of the territory of China.

vii. International treaties

336. Section 2.5 of each Data Transfer Assessment sets out TikTok Ireland's assessment of international agreements and related commitments concluded by China on handling of personal information to support the safeguarding of data.

337. In respect of international agreements, TikTok Ireland's 2021 and 2022 Data Transfer Assessments concluded that, while China provides some safeguards, it materially diverges from EU standards.

338. TikTok Ireland notes in Section 2.5 of the Data Transfer Assessments that although China has not entered into international treaties specifically on processing personal information, such as the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, it has:

(i) joined the Regional Comprehensive Economic Partnership together with 14 other Asia-Pacific Region countries, which recognises certain rules regarding personal information protection within the region,

(ii) joined the Global Data Security Initiative, as part of the Data Security Cooperation Initiative of China and Central Asia,

[152] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 131.
[153] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 189.

(iii) applied to join the Comprehensive and Progressive Trans-Pacific Partnership which requires all parties to adopt or maintain a legal framework protecting personal information,

(iv) applied to join the Digital Economy Partnership Agreement, which requires parties to adopt a legal framework considering international principles and guidelines and to adopt non-discriminatory practices in protection personal information,

(v) adopted Article 12 of the Personal Information Protection Law provides that China (i) will actively participate in the international rule-making on personal information protection and promote international cooperation on personal information protection, and (ii) will further facilitate the mutual recognition of personal information protection rules of other countries, regions or international organisations.

339. TikTok Ireland considers that while no EU Member States are a party to the international partnerships, initiatives and agreements described in Section 2.5 of the Data Transfer Assessments, China's participation in them, which contain rules on personal information protection (including with respect to government access), demonstrates China's commitment to personal data protection. TikTok Ireland has assessed, in this regard, that the Chinese legal framework contains some safeguards, but materially diverges from EU standards.

340. Again, TikTok Ireland considers, that in practice, the divergence does not present issues on the basis that its legal analysis is that the Chinese authorities do not have legal jurisdiction to compel organisations and individuals to provide data that are stored outside of the territory of China.

viii. Outcome of assessment at Section 2

341. As set out further below, TikTok Ireland determined in respect of transfers made pursuant to the 2010 SCCs and the 2021 SCCs, that:

(i) aspects of the Chinese legal framework, discussed above, preclude a finding of essential equivalence to EU law, even where SCCs are used, and

(ii) notwithstanding the various safeguards under the relevant legal framework in China, it was necessary and appropriate to adopt a range of supplementary measures in order to ensure the effectiveness of the SCCs.[154]

342. In respect of the outcome of its assessment in respect of the 2010 SCCs, TikTok Ireland was asked during the Inquiry to clarify and identify precisely which obligations in the 2010 SCCs and the Intra-Group Agreement that TikTok Ireland considered were at risk of being ineffective or not complied with in practice.

343. TikTok Ireland stated, in response to this query relating to the 2010 SCCs, that the supplementary measures were adopted in light of the controller's recognition in the Data Transfer Assessment that *"SCCs alone cannot provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law"*. Its position in respect of the 2010 SCCs was that:

> The Data Transfer Assessment made clear that there is a different legal system in China to that in the EU. TikTok identified in the Data Transfer Assessment certain areas where it could be perceived that China's laws may not provide essentially equivalent protection to that under EU Law. As set out in the

[154] TikTok Ireland's Response dated 12 October 2021, at page 3 and Data Transfer Assessment – China Group Entities dated 12 October 2021, at page 2, Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 2, Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 10.

Data Transfer Assessment, the adoption of supplementary measures should "ensure that any perceived risks….are minimised".

In the specific circumstances of the authorised remote access being assessed under the Data Transfer Assessment, TikTok considered that specific obligations in the 2010 SCCs were not at risk of being ineffective or not being complied with. Rather, the authorised remote access framework bolstered the level of protection afforded to the Transfers.

There is no impediment as a matter of Chinese law to the China Group Entities complying with their obligations under the 2010 SCCs in respect of the Transfers.

Consistent with this, the Data Transfer Assessment did not, in the specific circumstances of the authorised remote access being assessed under the Data Transfer Assessment, identify any specific obligations in the SCCs considered to be at risk. Nonetheless, the implementation of supplementary measures is considered by TikTok to reflect best practice, to be consistent with its commitment to privacy and security and to align with the measures set out in its Data Transfer Policy.[155]

344. It is expressly stated in the Data Transfer Assessments that TikTok Ireland considers that the current legal framework in China has issues that would preclude a finding of essential equivalence to EU law, even where SCCs are used.

345. TikTok Ireland considers that it complied with its obligation to assess the law and practices of China in the context of the transfers and to verify and guarantee and an essentially equivalent level of protection.

346. In respect of the position under the 2010 SCCs, TikTok Ireland submitted as follows:[156]

4.42 For the reasons explained above, TikTok has demonstrated that it has complied with its responsibility to assess the level of protection of EEA Users whose personal data is transferred by way of Remote Access to China Group Entities using the 2010 SCCs, in compliance with its obligations.

4.43 China Group Entities are in a position to comply with the 2010 SCCs and the Remote Access is granted in compliance with Chapter V GDPR. TikTok has demonstrated this to be the case, based upon a thorough assessment set out in the Data Transfer Assessment, as complemented by TikTok's responses in the Inquiry, that comprehensively assessed the nature and extent of the risk presented in the circumstances.

4.44 In considering Issue for Determination 3, TikTok respectfully requests that the DPC has appropriate regard to various important facts that were not referred to in Section V of the Statement of Issues, including the fact that Chinese authorities do not have the power to compel disclosure of

[155] TikTok Ireland's Response dated 20 June 2022, at page 17.
[156] TikTok Ireland's Submission dated 17 June 2022, at page 18.

the remotely accessible EEA User Data by the China Group Entities and, as a result, a China Group Entity would be entitled to reject a disclosure request for it.[157]

347. In respect of the position under the 2021 SCCs, TikTok Ireland has submitted that:[158]

> 5.8 Consistent with its position as outlined in Sections 4.42 to 4.44 and Section 5.24 of the September 2022 Response and for the reasons outlined in the September 2022 Response, as augmented by this Submission:
>
> 5.8.1. TikTok has demonstrated that it has complied with its responsibility to assess the level of protection of EEA Users whose personal data is transferred by way of Remote Access to China Group Entities using the 2021 SCCs, in compliance with its obligations.
>
> 5.8.2. The China Group Entities are in a position to comply with the 2021 SCCs and the Remote Access is granted in compliance with Chapter V GDPR. TikTok has demonstrated this to be the case, based upon a thorough assessment set out in the Updated Data Transfer Assessment, as complemented by TikTok's responses in the Inquiry, that comprehensively assessed the nature and extent of the risk presented in the circumstances.
>
> 5.8.3. In considering Issue for Determination 3, TikTok respectfully requests that the DPC has appropriate regard to various important facts that were not referred to in Section V of the Statement of Issues, including the fact that Chinese authorities do not have legal power under Chinese law to compel disclosure of the remotely accessible EEA User Data and that a China Group Entity will not provide EEA User Data in all cases.
>
> 5.8.4. TikTok has demonstrated that supplementary measures implemented by TikTok and the China Group Entities in respect of the Remote Access by the China Group Entities to EEA User Data are effective, together with the 2021 SCCs, to ensure an essentially equivalent level of protection.
>
> 5.9 In considering the above, TikTok respectfully submits that the DPC should also have regard to the updated facts arising from the transition to the 2021 SCCs and the new and updated supplementary measures that are now in place.

d) Analysis as to TikTok Ireland's compliance with its obligation to assess the law and practices in effect in China regarding the level of protection of personal data of EEA users the subject of the Data Transfers

348. Each of TikTok Ireland's Data Transfer Assessments identified that Chinese law and practices do not provide safeguards essentially equivalent to the European Union in respect of regulation of data privacy, regulation of public authority access to personal data, regulatory supervision, right of redress, and International treaties. The Assessments identified that Chinese law and practices diverge from the European Essential Guarantees.

---

[157] As noted above, the DPC furnished TikTok Ireland with a Statement of Issues in the Inquiry on 7 July 2022 and TikTok Ireland, having been granted an extension of time, furnished its submission on the Statement of Issues on 15 September 2022.

[158] TikTok Ireland's Submission dated 19 December 2022, at page 8.

349. TikTok's 2021 and 2022 Assessments concluded that the divergences do not undermine the safeguards provided on the basis that Chinese authorities are not lawfully entitled to compel organisations and individuals to provide data that are not domestically stored within the territory of China. These assessments relied on the territoriality principle in coming to the conclusions that 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. TikTok Ireland's assessments set out that *"Chinese law recognises the general principle of sovereignty, such that the scope of application of a country's law is limited to its territory. Unless there are specific and express exceptions regarding extra-territorial application of Chinese laws, Chinese laws are subject to territoriality principle, particularly administrative laws."*[159]

350. The Second Xu Report further elaborated on the territoriality principle and described it as follows:

> The territoriality principle means that the government regulates acts occurring within its own territory. This is based on the principle of sovereign equality of States in the PRC Constitution which is widely recognized in various Chinese laws.[160]

351. The DPC's Preliminary Draft Decision set out that TikTok Ireland failed to comply with its responsibility to adequately assess the level of protection of EEA Users under the Chinese legal framework on the basis of its failure to appropriately consider how the territoriality principle applies in the context of the divergences in the Chinese legal framework from EU standards that TikTok Ireland acknowledges exist. The DPC's Preliminary Draft Decision also provisionally found that TikTok Ireland's analysis did not set out in a clear way the deficiencies it acknowledges exist in the Chinese legal framework.

352. In the Preliminary Draft Decision, the DPC set out two concerns regarding TikTok Ireland's conclusion with regard to the effect of the territoriality principle in Chinese law.

353. The first concern related to how laws such as the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law or the National Intelligence Law may be interpreted to have extra-territorial effect and 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 Entities.

354. The second concern related to the basis for TikTok's conclusion regarding the application of the territoriality principle in the specific factual context of the Data Transfers. In the Preliminary Draft Decision, the DPC provisionally found that TikTok Ireland failed to verify, guarantee and demonstrate the adequacy of the protection in respect of the Data Transfers as it had furnished insufficient information in the Inquiry to support the conclusion that the territoriality principle does in fact operate so as to prevent the application of problematic laws to the personal data of EEA Users the subject of the transfers, save in situations where those laws have extra-territorial effect. This concern was based on two issues as identified in the Preliminary Draft Decision:

(i) TikTok Ireland's failure to demonstrate that the China Group Entities and their employees in China would fall outside of the scope of the problematic laws, and

(ii) The vagueness with which TikTok Ireland had described in its Data Transfer Assessments and its submissions as to the exact contours of the territoriality principle. In particular, the DPC highlighted that TikTok Ireland did not refer to legal authorities that interpret the territoriality

[159] TikTok Ireland's Data Transfer Assessment, 13 October 2022, at page 19.
[160] The Second Xu Report at page 6.

principle in practice in a scenario concerning remote access, using technical means, by persons within the jurisdiction of China to data stored on servers in a foreign jurisdictions.

355. As a result of those concerns, the DPC provisionally concluded in the Preliminary Draft Decision that:

> Both of those concerns mean that [the DPC is] not satisfied, in light of TikTok Ireland's submissions, to conclude definitively that problematic laws such as the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law and National Intelligence Law could not apply in practice to the transfers the subject matter of this Inquiry save in the exceptional circumstances where they would in interpreted to have extra-territorial effect. [The DPC considers] that there is a lack of clarity regarding the territoriality principle in Chinese law, and in how the surveillance laws referred to in Section 2.2 of the Data Transfer Assessments may in fact apply in the context of the transfers, a matter which [the DPC] consider[s] to be of significant concern.[161]

356. The 2021 and 2022 Data Transfer Assessments each advanced the proposition that the import of the territoriality principle in Chinese law means that the Data Transfers fall outside the territorial scope of the surveillance laws.

357. Following the Preliminary Draft Decision, TikTok Ireland submitted additional information to the Inquiry seeking to demonstrate the basis for its conclusion that the Data Transfers fall outside the territorial scope of surveillance laws. TikTok Ireland continued to make further submissions to the Inquiry. TikTok Ireland's 2023 Data Transfer Assessment was created after the DPC's Preliminary Draft Decision. While this document was compiled following the end of the temporal scope of the Inquiry, it provided additional information to support the company's conclusion in the 2021 and 2022 assessments that the Data Transfers fall outside the territorial scope of surveillance laws. The 2023 Data Transfer Assessment included the following assessment on the legal jurisdiction of Chinese authorities to compel disclosure of remotely accessible EEA User Data:

> As set out in Section 2.2B(3), a Chinese authority must have both adjudicatory jurisdiction and enforcement jurisdiction to be able to compel a China Group Entity or one of their personnel in China to disclose the remotely accessible EEA User Data.
>
> Where Chinese law does exceptionally provide for extraterritorial effect such that foreign entities or individuals may fall within the scope of the adjudicatory jurisdiction of Chinese law, this does not mean that a Chinese authority has the power to exercise enforcement jurisdiction to compel the disclosure of data stored outside China. Rather, it simply means that the Chinese authority has exercised its legislative jurisdiction to provide adjudicatory jurisdiction to investigate and prosecute the relevant occurrence.
>
> **(i) Normally no adjudicatory jurisdiction**
>
> A Chinese authority normally would not have adjudicatory jurisdiction to obtain EEA User Data in the first place. This is because:

[161] DPC Preliminary Draft Decision at paragraph 258. The PDD was expressed in the first person of the Commissioner for Data Protection. With the expiry of the Commissioner's term of office, two new Commissioners were appointed on 20 February 2024. For ease of reference references to a one-Commissioner DPC in 2023 has been replaced in the decision with references to a two Commissioner DPC or simply "the DPC".

- as set out in Section 2.2B(3), under Chinese law what businesses or individuals residing outside China do is generally not regulated by or within the adjudicatory jurisdiction of Chinese law; and

- EEA User Data is generated and collected by TikTok in its business that is not linked or relevant to China and EEA User Data relates to individuals residing outside China.

However, as set out in Section 2.2B there are certain limited laws that expressly provide for extraterritorial adjudicatory jurisdiction (such as the Criminal Law, which may be applicable to non-Chinese citizens who commit a crime outside the territory of China against China or Chinese citizens) so that occurrences outside China could, in theory, fall within the adjudicatory jurisdiction of a Chinese authority, provided that the relevant occurrence had a specific connection to China and the lawful rights and interests of China or Chinese citizens were infringed. This is likely to arise in extremely limited circumstances in the specific circumstances of the transfers given that, as set out above, EEA User Data is generated and collected by TikTok in its business that is not linked or relevant to China and EEA User Data relates to individuals residing outside China. Nonetheless, it cannot be entirely ruled out.

(ii) No enforcement jurisdiction in any event

Under Chinese law, a Chinese authority would only be able to compel an entity or person in China to disclose data stored in a foreign State if it had been expressly granted extraterritorial enforcement jurisdiction.

As set out in Section 2.2B(3), none of the limited and exceptional Chinese laws discussed in this Assessment with extraterritorial adjudicatory jurisdiction grant extraterritorial enforcement jurisdiction that would enable Chinese authorities to compel a China Group Entity or one of their personnel in China, or TikTok, to disclose the remotely EEA User Data stored in the US, Singapore or Malaysia. This would apply even in the unlikely case that a Chinese authority had adjudicatory jurisdiction in a given case.

(iii) Chinese authorities must follow a mutual judicial assistance process or other diplomatic channels

As set out in Section 2.2B(3), there is a legal requirement for a Chinese authority to follow a mutual judicial assistance process or other diplomatic channel in order to enforce the law against foreign entities or individuals and/or obtain data stored outside China.

Consequently, in the specific circumstances of the transfers through the Remote Authorised Access, China Group Entities are entitled to not provide the remotely accessible EEA User Data in all cases.

This conclusion is consistent with the independent expert opinion of Professor Xu, an expert in Chinese law, which is annexed to this Assessment at Appendix B.

…

(v) Documented practical experience

The above assessment is consistent with the practical experience as set out at Section 2.2B(3)(vi). This includes the documented practical experience of the China Group Entities as well as Professor Xu's and Clifford Chance's experience (see annexed reports at Appendices B and C respectively) who have

confirmed that they are not aware of Chinese authorities compelling disclosure of data stored outside China in practice.

The China Group Entities' experience accords with public statements by the Chinese Government (see Section 2.2B(10)), e.g.:

"China has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government by installing 'backdoors' or by violating local laws".

2.6(4) Right of redress

EEA Users have necessary enforceable data subject rights and effective legal remedies available to them in respect of the remotely accessible EEA User Data.

As outlined above, a China Group Entity cannot be compelled to disclose EEA User Data. As a result, an EEA User would not have any reason to want or need to exercise their right of redress. This is the case even in the unprecedented and unlikely event that a request were to be made on a confidential basis as a China Group Entity cannot be compelled to disclose the EEA User Data.

This is consistent with the conclusion in Section 2.4A(2) that there is essentially equivalent protection under Essential Guarantee D for transfers made by remote access to data stored outside China.

Furthermore, TikTok, as controller, is accountable under the GDPR to EEA Users (including under Articles 79 and 82 GDPR) for the processing by it and its processors and sub-processors, including the China Group Entities. EEA Users can exercise their right to an effective judicial remedy in this regard before the Irish courts or the courts of their home Member State. EEA Users also have the right to complain under the GDPR to, in particular, the DPC or supervisory authority of their home Member State with respect to the processing of EEA User Data by or on behalf of TikTok, including by the China Group Entities, and to be kept informed of the progress and outcome of the complaint.

EEA Users also have enforceable data subject rights and effective legal remedies available to them as third party beneficiaries under the SCCs, which are governed by Irish law. The SCCs were designed to specifically address concerns raised in the Schrems II case (C- 311/18). As stated in Clause 2(a), the "[2021 SCCs] set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c)" of the GDPR.

If an EEA User invokes a third party beneficiary right under the SCCs, he/she may lodge a complaint with the DPC or the supervisory authority in the Member State of their habitual residence or refer the dispute to the Courts of that Member State or Ireland. Legal proceedings to enforce their rights and remedies under the SCCs can be brought against both TikTok and the China Group Entities.

Under the SCCs, the China Group Entities submit themselves to the jurisdiction of the DPC and agree to cooperate with the DPC in any procedures aimed at ensuring compliance with the SCCs. In particular, the China Group Entities agree to respond to enquiries, submit to audits and comply with the measures adopted by the DPC, including remedial and compensatory measures. They also agree to provide the DPC with written confirmation that the necessary actions have been taken. This includes

where an EEA User submits a complaint to the DPC or the supervisory authority in the Member State of their residence.

Under the SCCs, the China Group Entities are liable to EEA Users, and EEA Users are entitled to receive compensation, for any material or non-material damages that they cause an EEA User by breaching the third-party beneficiary rights under the SCCs. In addition, TikTok is liable to EEA Users, and EEA Users are entitled to receive compensation, for any material or non-material damages TikTok or a China Group Entity causes an EEA User by breaching the third-party beneficiary rights under the SCCs. This is without prejudice to the liability of TikTok under the GDPR. Where TikTok and a China Group Entity is responsible for any damage caused to an EEA User as a result of a breach of the SCCs, they are jointly and severally liable and the EEA User is entitled to bring an action in court against any of them.

The China Group Entities specifically confirm that they will abide by a decision that is binding under the applicable EU or Member State law (and, as companies belonging to the same corporate group as TikTok, there is no concern that a China Group Entity would not do so as a matter of practice). The China Group Entities also accept that an EEA User may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR. In this way, the SCCs facilitate individual redress and ensure effective enforcement.

Further, EEA Users do have a high level of enforceable data subject rights and effective legal remedies available to them under Chinese law when it comes to transfers where the data is stored on servers in China.

2.6(5) Conclusion

In conclusion, the assessment in this Section 2 demonstrates that the adopted form of transfer mechanism effectively ensures that the transferred data will be afforded a level of protection in China that is essentially equivalent to that guaranteed in the EEA.

This conclusion is contingent on the transfers being implemented by way of remote access to EEA User Data stored outside China. It is recommended that appropriate supplementary measures for this are implemented accordingly. The Supplementary Measures are considered in Section 3.[162]

358. Following the Preliminary Draft Decision, TikTok Ireland made further submissions and submitted the Second Xu Report. The report puts forward Professor Ke Xu's opinion on two questions:

(i) Whether Chinese authorities have the power to compel China Group Entities (or their personnel in China) to disclose remotely accessible EEA User Data that is stored on servers outside China ("Question 1").

(ii) Whether the statement of Chinese law contained in Section 2 of the Data Transfer Assessment for China (December 2022), which was submitted by TikTok to the DPC in the

[162] TikTok Ireland's Data Transfer Assessment, dated October 2023, at pages 106-111.

Inquiry, is an accurate statement of Chinese law as at December 2022 and is consistent with the views expressed in this expert opinion regarding the Question 1 ("Question 2").

359. The Second Xu Report contends that the territoriality principle in Chinese Law means that the government regulates acts occurring within its own territory alone. It states that this is based on the principle of sovereign equality of States in the PRC Constitution which is widely recognised in various Chinese laws. The Report states that the territoriality principle constitutes a substantial constraint on Chinese authorities' cross-border access to data and is reflected in Chinese policies and initiatives.

360. The Second Xu Report sets out how jurisdiction in Chinese Law comprises at least three different aspects: legislative jurisdiction[163], adjudicative jurisdiction[164], and enforcement jurisdiction.[165] The Second Xu Report emphasises the distinction between adjudicatory jurisdiction and enforcement jurisdiction as follows:

> To take an example, a State may confer adjudicatory jurisdiction on an authority or Court in respect of occurrences outside the State, but doing so does not necessarily confer enforcement jurisdiction on an authority to compel someone outside the State to undertake particular acts even where related to a matter in respect of which the authority or a Court has adjudicatory jurisdiction. There is a distinction between adjudicatory and enforcement jurisdiction.

361. The Second Xu Report sets out how, if a Chinese law does provide for extraterritorial effect such that foreign entities or individuals may fall within the scope of the adjudicatory jurisdiction of Chinese law, this does not mean that a Chinese authority has the power to exercise enforcement jurisdiction to compel the disclosure of data stored outside China. Rather, it simply means that the Chinese authority has exercised its legislative jurisdiction to provide adjudicatory jurisdiction to investigate and prosecute the relevant occurrence.

362. The Second Xu Report also refers to how certain Chinese laws, like the Criminal Law, expressly confer adjudicatory jurisdiction with respect to acts occurring outside the territory of China. However, the report outlines that it does not follow that these laws confer jurisdiction on the Chinese authorities to carry out intelligence gathering or investigative activities in a foreign State. This would constitute the exercise of *"enforcement jurisdiction"* in a foreign State, which is generally prohibited as a matter of international law, save where authorised by a rule derived from international custom or from a convention.

363. The Second Xu Report outlines how the adjudicatory jurisdiction granted by the following Chinese laws does not grant extraterritorial enforcement jurisdiction:

(i) Articles 8 and 9 of the Criminal Law,

(ii) Article 75 of the Cybersecurity Law,

(iii) Article 11 of the Anti-Terrorism Law, and

[163] The report describes legislative jurisdiction as the power of a State to legislate against persons, things, and conduct.
[164] The report describes adjudicative jurisdiction as the power to subject persons, things, and conduct to judicial process.
[165] The report describes enforcement jurisdiction as compelled compliance in accordance with the law.

(iv) Article 10 of the Counter-Espionage Law.

364. The basis for this conclusion in the Second Xu Report is that adjudicatory jurisdiction does not itself grant extraterritorial enforcement jurisdiction and compelling a person to disclose 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. The report concludes that this would infringe the sovereignty of the foreign State.

365. Regarding Article 10 of the National Intelligence Law, the Second Xu Report stated that this law does not contemplate extraterritorial adjudicatory effect.[166] The report also stated that Article 10 does not by itself confer or establish any power or enforcement jurisdiction that enables Chinese national intelligence agencies to compel an entity or individual in China or abroad to provide data in China or abroad.

366. TikTok Ireland updated the 2023 Data Transfer Assessment to include a table that set out how, in respect of the transfer by remote access:

(i) Adjudicatory Jurisdiction is unlikely for the Criminal Law and Criminal Procedure Law, Anti-Terrorism Law, Counter-Espionage Law, and Cybersecurity Law. Adjudicatory Jurisdiction does not exist for the National Intelligence Law.

(ii) Enforcement Jurisdiction does not exist for each of the Criminal Law and Criminal Procedure Law, National Intelligence Law, Anti-Terrorism Law, Counter-Espionage Law, and Cybersecurity Law.

(iii) Diplomatic channels must be followed to obtain data for the Criminal Law and Criminal Procedure Law, National Intelligence Law, Anti-Terrorism Law, Counter-Espionage Law, and Cybersecurity Law.

367. The Second Xu Report concluded that:

> …in order for a Chinese authority to obtain data stored outside China, three cumulative conditions must be met: (1) the Chinese authority must, by virtue of special provisions on "protective jurisdiction", have extraterritorial adjudicatory jurisdiction over a matter in respect of which the data is relevant; (2) the Chinese authorities must act in accordance with the authority and procedures prescribed by Chinese laws in relation to criminal activities and the administrative enforcement activities, which will be illustrated in more details in 3.1 and 3.2 below; and (3) the Chinese authorities must act in accordance with international treaties or bilateral arrangements or memoranda in order to obtain the data.

368. The Second Xu Report concluded as follows in respect of the questions:

> **Question 1**
>
> In the specific circumstances of the transfers the subject of the Inquiry, Chinese authorities do not have unilateral administrative power to compel disclosure by China Group Entities, or personnel in China working for them, of EEA User Data stored outside China (i.e. in Singapore, US, or Malaysia) which they can remotely access, even in the exceptional cases where Chinese laws prescribe extra territorial adjudicatory jurisdiction. Instead, Chinese authorities would have to obtain EEA User Data stored outside China through cooperation with the relevant foreign State.

[166] Unlike Articles 8 and 9 of the Criminal Law, Article 75 of the Cybersecurity Law, Article 11 of the Anti-Terrorism Law, and Article 10 of the Counter-Espionage Law.

> In practice, I am unaware of any cases where Chinese authorities have compelled, or sought to compel, an entity or individual in China to disclose data that is stored outside China in a foreign State.
>
> **Question 2**
>
> In response to Question 2, this expert opinion holds the view that the statement of Chinese law contained in Section 2 of the Data Transfer Assessment for China (December 2022), which was submitted by TikTok to the DPC in the Inquiry, is an accurate statement of Chinese law as at December 2022 and is consistent with the views expressed in this expert opinion regarding Question 1.

369. Following the Preliminary Draft Decision, TikTok Ireland also submitted an expert report dated 8 September 2023 of a leading Chinese law firm, Fangda Partners ('**Fangda Report**')[167]. The report states that it is an opinion in response to the Preliminary Draft Decision. The report stated that:

> I confirm that the statement of Chinese law contained in Section 2 of the Data Transfer Assessment (December 2022) is an accurate statement of Chinese law as of December 2022.

370. The Fangda Report considered the changes in Chinese law since the 2022 Data Transfer Assessment and concluded that the amendments identified did not materially change the analysis and statement of Chinese law contained in Section 2 of the 2022 Data Transfer Assessment.

371. Following the Preliminary Draft Decision, TikTok Ireland also submitted an expert report, again dated 8 September 2023, prepared by Clifford Chance ('**Clifford Chance Report**')[168], an international law firm located in China. This report stated:

> In our experience of providing services to clients as well as our observations as an international law firm in China, we have not seen PRC authorities compel or take enforcement action seeking to compel PRC Persons, to disclose data stored with or by another entity (affiliated or not) outside China, including data stored outside China which is remotely accessible by PRC Persons in China.

372. TikTok Ireland's submissions in response to the Preliminary Draft Decision concluded as follows on the operation of the territoriality principle as a matter of Chinese law:

---

[167] The Fangda Report was created by Gil Yi Zhang, who was described in the report as a practicing attorney-at-law registered in the People's Republic of China ("PRC") and a partner in the Shanghai office of Fangda Partners, one of China's leading law firms. The report set out that Gil Yi Zhang was retained by TikTok Ireland to assist it with the preparation of the Data Transfer Assessment and in the course of the Inquiry. The Report also set out that Fangda Partners is a full-service law firm advising on PRC laws and has extensive practical experience in data protection, cyber security, cross border transfer of data, big Data and artificial intelligence. The report sets out that Gil Yi Zhang specialises in data protection matters, cyber security, and regulatory compliance and has practiced in private practice and in-house as senior counsel for many years.

[168] The Clifford Chance Report did not state the name of its author. The report set out that Clifford Chance LLP is amongst the largest international law firms operating in China. The report stated that the firm's teams regularly advise leading global companies on matters of data protection and cybersecurity law.

1) EEA User Data is not stored on servers in China. It is instead stored on servers in the United States, Singapore and Malaysia.[169]

2) While data stored in China is subject to Chinese jurisdiction, Chinese law recognises data stored on a foreign server as subject to the sovereign jurisdiction of that foreign State. This is based on well-established principles of territoriality and sovereignty.

3) A Chinese authority, should it wish to compel a China Group Entity or one of its personnel to disclose EEA User Data, would, in technical terms, need to compel the China Group Entity / individual to perform acts (i.e. remotely access data) in the United States, Singapore or Malaysia in order to facilitate this.

4) Under Chinese law, compelling a domestic person to perform acts in a foreign State to disclose data stored in that foreign State violates the foreign State's sovereignty – the acts of the individual in the foreign State are effectively attributed to the State compelling them to perform the relevant acts.

5) In the same way that China prohibits foreign authorities, entities and individuals from accessing data stored in China for evidence collection unless authorised by a competent Chinese authority (as a matter of Chinese sovereignty), China applies the same prohibition in reverse to Chinese authorities that wish to access data stored in a foreign State.

6) This means that Chinese authorities cannot collect (whether from someone in or outside China) data located in a foreign State, unless authorised by a competent foreign State authority.

7) Chinese authorities are therefore required, in practice, to follow mutual legal assistance or other diplomatic processes to access data located in a foreign State.

8) Chinese law is not unique in recognising that a State infringes a foreign State's sovereignty when it compels a person in its territory to perform acts in the territory of that foreign State. This is a well-established principle of international law.

9) Under Chinese law, an authority would only be able to do this if it has been expressly granted extraterritorial enforcement jurisdiction as a matter of law.

10) Whilst certain limited and exceptional Chinese laws like the Criminal Law apply to acts occurring outside the territory of the State (*"adjudicatory jurisdiction"*), it does not follow that these laws confer jurisdiction on the Chinese authorities to carry out intelligence gathering or investigative activities in a foreign State. This would constitute the exercise of *"enforcement jurisdiction"* in a foreign State, which is generally prohibited as a matter of international law, save where authorised by a rule derived from international custom or from a convention.

[169] While TikTok Ireland no longer maintains that EEA User Data was not stored on servers in China during the temporal scope, the material scope of this Decision is limited to transfers that occurred by means of remote access to EEA User Data stored on servers outside of China.

11) None of the limited and exceptional Chinese laws identified with extraterritorial adjudicatory jurisdiction grant enforcement jurisdiction that would enable Chinese authorities to compel access to data stored in a foreign State. This is consistent with the Chinese government's policy that Chinese authorities and other States should not do so.[170]

373. The DPC has considered all information submitted by TikTok Ireland during the Inquiry regarding the territoriality principle. This includes the Legal Opinions, the updated Data Transfer Assessments, and the submissions made after the Preliminary Draft Decision. However, for the reasons set out below, the DPC finds that TikTok Ireland has failed, on a continuing basis, to adequately assess the level of protection of EEA Users under the Chinese legal framework in respect of the territoriality principle and the divergences that TikTok Ireland acknowledges to exist. In particular, TikTok Ireland failed to adequately assess the law and practices in effect in China regarding the level of protection of personal data of EEA Users the subject of the Data Transfers.

374. The submissions submitted by TikTok Ireland following the Preliminary Draft Decision include additional relevant information on the territoriality principle in Chinese law and the ability of Chinese authorities to compel organisations and individuals in China to provide data that is located in another jurisdiction. In particular, the Second Xu Report addresses the concern that the Anti-Terrorism Law, Counter-Espionage Law, Cybersecurity Law or the National Intelligence Law may be interpreted to have extra-territorial effect. While some of these laws may grant extraterritorial adjudicatory jurisdiction, the Second Xu Report outlines that none of them grant extraterritorial enforcement jurisdiction, and consequently asserts that these laws cannot be used by Chinese authorities to compel access to personal data while that data is located outside of China. Therefore, this legal opinion addresses the risk of these laws being used by Chinese Authorities to request disclosure of EEA User Data while that data is not located in China.

375. While the information submitted by TikTok Ireland after the Preliminary Draft Decision addresses the concern of the Problematic Laws being applied to EEA User Data while that data is located outside of China, TikTok Ireland has continually failed to address the application of those laws to the processing of EEA User Data that does occur on computer information systems in China by means of the Remote Access Solution. For the reasons that follow, the DPC finds that TikTok Ireland has continually failed to establish that the territoriality principle does in fact operate so as to prevent the application of problematic laws in practice to the particular transfers the subject matter of this Inquiry in China by means of the Remote Access Solution.

376. Accordingly, the DPC's second concern as set out in the Preliminary Draft Deicsion regarding TikTok Ireland's conclusion with regard to the effect of the territoriality principle in Chinese law remains, despite the extensive information submitted by TikTok Ireland following the Preliminary Draft Decision. TikTok Ireland has continually failed to demonstrate that the China Group Entities and their employees in China would fall outside of the scope of the problematic laws. It has also continually failed to set out with clarity the exact contours of the territoriality principle, and has continually failed to refer to authorities that interpret the territoriality principle in practice in a scenario concerning remote access, using technical means, by persons within the jurisdiction of China. Therefore, the two issues giving rise to the second concern articulated in the Preliminary Draft Decision remain.

377. TikTok Ireland has not established that EEA User Data, the China Group Entities or their employees fall outside the scope of problematic laws when EEA User Data is transferred to China. Furthermore, TikTok Ireland has failed to refer to any legal authorities that interpret the territoriality principle in practice in respect of EEA

[170] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at pages 64 and 65.

User Data that is transferred to China. Instead, TikTok Ireland has focused on the EEA User Data in the context of its storage on servers outside of China, and has not considered the application of the territoriality principle to the personal data while that data is processed in China. TikTok Ireland has not advanced any other argument to establish how EEA User Data are not within the scope of problematic laws in China, which TikTok Ireland itself describes in its Data Transfer Assessments.

378. 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.

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.

381. Therefore, the conclusion in the Fangda Report that confirms, *"that the statement of Chinese law contained in Section 2 of the Data Transfer Assessment (December 2022) is an accurate statement of Chinese law as of December 2022"* and the amendments to Chinese law since the 2022 Data Transfer Assessment did not materially change this analysis, also overlooks this issue.

382. TikTok Ireland's Data Transfer Assessments identified divergences from European Essential Guarantee A, B, C and D. It also identified divergences in terms of the extent to which China has concluded international treaties and related commitments on handling of personal information to support the safeguarding of data. The conclusions in sections 2.1, 2.2, 2.3, 2.4, and 2.5 of the December 2022 Assessment regarding how the divergences identified in each of those sections does not result in a lack of essentially equivalent protection relies on the following position that is repeated in each Section:

> …Chinese authorities are not lawfully entitled to compel organisations and individuals to provide data that are not domestically stored within the territory of China. Consequently, this divergence [in safeguards] does not undermine the effectiveness of the contractual safeguards contained in the SCCs with respect to such data.[171]

383. TikTok Ireland's assessments, submissions and the Second Xu Report have considered the territoriality principle in significant detail in respect of this conclusion. While TikTok Ireland has expressly addressed the

[171] TikTok Ireland's Data Transfer Assessment, dated December 2022, at pages 12, 27, 44, 55, and 63.

potential for Chinese authorities to compel access to EEA User Data when it is stored on servers located outside of China, it has failed to consider how Chinese law and practices apply in respect of the personal data that is transferred to China. TikTok Ireland's conclusion in its Data Transfer Assessments failed to consider the processing of personal data that does occur within the territory of China. TikTok Ireland's submissions to the Inquiry also establish that a significant amount of personal data was routinely subject to the Remote Access Solution for purposes such as content delivery, security, research and development, analytics, online payments, customer and technical support, and content moderation. The nature of this processing was equally broad and concerned diverse matters relating to monitoring content trends, testing, and protecting the platform from fraudulent payments. As set out in the Data Transfer Assessments dated 12 October 2021 and 13 October 2022, this results in a broad range of categories of personal data being transferred to China.

384. TikTok Ireland's assessment of the Chinese legal framework appears to assume that the only potential form of problematic access to this data could occur by means of Chinese authorities compelling access to EEA User Data exclusively when it is stored on servers located outside of China. However, this overlooks the question of Chinese authorities obtaining access to the personal data that was routinely transferred to China and that was temporarily processed there to facilitate the remote access. TikTok Ireland's assessment of the law and practices in China did not establish that the territoriality principle prohibits such access while the personal data was being routinely transferred to China. Chinese authorities accessing such data would not be contingent upon compelling an individual to access data on foreign server where that data is, at that time, located on computer information systems in China. In particular, TikTok Ireland did not consider how the territoriality principle in Chinese law would interact with the potential for Chinese authorities to obtain personal data directly or indirectly from computer information systems located in China that process EEA User Data as part of the remote access.

385. Therefore, the practical experience put forward in the Clifford Chance Report that the authors had not seen PRC authorities compel or take enforcement action seeking to compel PRC Persons, to disclose data stored with or by another entity (affiliated or not) outside China, including data stored outside China which is remotely accessible by PRC Persons in China, also does not consider this potential form of access.

386. The DPC notes that the first question that Professor Xu was asked to answer by TikTok Ireland by means of the Second Xu Report was whether Chinese authorities have the power to compel China Group Entities (or their personnel in China) to disclose remotely accessible EEA User Data that is stored on servers outside China. The question put to Professor Xu focused on data that is not located in China. As a result, the Second Xu Report does not consider the potential for access to EEA User Data when that personal data is located in China. For example, the Second Xu Report's consideration of the Rules for Electronic Data Evidence states:

> Article 23 of Rules for Electronic Data Evidence restricts the power to extract data online to the extent that only data already publicly available or data stored on computer information systems within the territory of China can be extracted; so it does not permit access to data stored outside China.[172]

387. The Second Xu Report does not consider how Chinese law and practices apply to the processing of EEA User Data as it is processed on computer information systems in China. Its assessment is limited to personal data when it is located outside of China only.

388. TikTok Ireland's position is that it does not consider that the use of its Remote Access Solution results in any *"storage"* of EEA User Data in China.[173] TikTok Ireland's definition of *"storage"* is premised on providing *"a*

[172] The Second Xu Report, at page 29.
[173] TikTok Ireland letter to the DPC dated 11 March 2024.

location for data when it is not being used, so that it can be later retrieved for any purpose." It relies on definitions of *"storage"* in the Oxford English Dictionary *"the action of storing or laying up in reserve"* or store *"a stock of anything… laid up for future use"*; and the (ii) Collins Dictionary *"If you refer to the storage of something, you mean that it is kept in a special place until it is needed"*. On that basis, TikTok Ireland does not consider that the processing carried out in China in connection with the Remote Access Solution is storage or a storage solution.

389. Irrespective of whether the processing of EEA User Data on computer information systems in China constitutes storage, temporary storage, or neither, TikTok Ireland's assessment of Chinese law and practices, including the territoriality principle, does not establish that this personal data cannot be subject to problematic access by Chinese public authorities. Its assessment did not submit any information that addresses how the application of the territoriality principle is relevant in the specific factual context of EEA User Data that is transferred to China by means of the Remote Access Solution and processed by the China Group Entities there.

390. TikTok Ireland's Data Transfer Assessments and its submissions to the Inquiry have addressed the potential of Chinese Authorities compelling the China Group Entities to access and disclose personal data stored on servers in Singapore, Malaysia, the United States and the European Economic Area, i.e. the ability of Chinese Authorities to access the EEA User Data while that data is located outside China. TikTok Ireland has set out how such access would be unlawful as a matter of Chinese law because it would involve Chinese Authorities enforcing jurisdiction beyond the territorial boundaries.

391. However, TikTok Ireland's transfers of EEA User Data to China by means of the Remote Access Solution routinely involves such personal data being processed in China. TikTok Ireland's assessment of Chinese law, including the territoriality principle, did not provide any analysis of the potential for Chinese authorities to access such data while it is temporarily processed in China. This form of access is distinct from Chinese authorities seeking to compel access to personal data while it is not within the territory of China, for example, data that is stored on servers outside of China before being subject to processing in China.

392. Therefore, the DPC's concerns as documented in the Preliminary Draft Decision regarding the effect of the territoriality principle in Chinese law remain, despite the additional information submitted by TikTok Ireland. While TikTok Ireland, in its submissions on the Preliminary Draft Decision, has further addressed the concern regarding the extraterritoriality of the problematic laws, it has failed to address the DPC's concern regarding the insufficient information submitted by TikTok Ireland to support TikTok Ireland's conclusion that the territoriality principle does in fact operate so as to prevent the application of problematic laws to the personal data of EEA Users the subject of the transfers, i.e. the personal data that is routinely transferred to China further to the Remote Access Solution. TikTok Ireland has not established that EEA User Data, the China Group Entities or their employees fall outside the scope of problematic laws when EEA User Data is transferred to China. Furthermore, TikTok Ireland has failed to refer to any legal authorities that interpret the territoriality principle as it operates in practice in China in respect of EEA User Data that is transferred to China.

393. These transfers occur by means of remote access and TikTok Ireland has failed to establish that the territoriality principle limits the potential for Chinese authorities to access EEA User Data when it is processed within the territory of China. In particular, TikTok Ireland has continually failed to refer to any authority that interprets the territoriality principle in practice in a scenario concerning remote access, using technical means, by persons within the jurisdiction of China to data stored on servers in a foreign jurisdiction, which results in that data being processed locally on computer information systems in China.

394. TikTok Ireland's response to the Preliminary Draft Decision stated:

> Chinese law treats data stored in China as subject to Chinese jurisdiction, and data that is stored in a foreign State's territory as subject to that foreign State's sovereign jurisdiction. As such, Chinese law

and policy regarding cross-border data access focuses on where the data is stored (and not, for instance, the location of the person to whom the request is made).[174]

395. While TikTok Ireland's submissions considered in detail how Chinese law's respect for data sovereignty applies to data as it is stored outside of China, it failed to consider the application of the territoriality principle in the specific context of the Data Transfers and how those transfers involve the processing of EEA User Data on computer information systems located in China.

396. In addition to the shortcomings in TikTok Ireland's assessment of the territoriality principle, TikTok Ireland's assessment also failed to set out in a clear way the deficiencies it acknowledged to exist in the Chinese legal framework. Having failed to establish that the territoriality principle prevents Chinese authorities from accessing EEA User Data when it is processed in China, TikTok Ireland ought to have assessed the scope of the divergences from EU standards, and the extent of the resulting risk to the protection of personal data of EEA Users. TikTok Ireland's analysis ought to have set out in a clear way the deficiencies it acknowledged to exist in the Chinese legal framework and the resulting risk in respect of the specific processing of EEA User Data subject to the Data Transfers.

397. However, where TikTok Ireland acknowledged the lack of equivalence of Chinese law with that of EU law, it failed to clearly define what it understood to be the scope of those divergences, and the extent of the resulting risk to the protection of personal data of EEA Users. This is a necessary exercise for a data controller to conduct in respect of the specific transfers that it undertakes in order to prevent unlawful data transfers under the GDPR. Where TikTok Ireland identified divergences in law and practice in China from law and practices in the EU, it did so in general terms only. It failed to provide sufficient consideration to how those divergences could apply to EEA User Data subject to the Data Transfers. The manner in which TikTok Ireland analysed the Problematic Laws did not clearly define what it understood to be the scope of the divergence from EU standards and the extent of the resulting risk to the protection of personal data of EEA Users.

398. TikTok Ireland's Data Transfer Assessments[175] set out the general legal framework for protection of personal data in China, including a detailed summary of the legal framework in China that is set out in each of those Data Transfer Assessments. However, the analysis failed to clearly outline the nature and extent of the divergence in equivalence between EU law and the law of China both prior to, and subsequent to, the adoption of the Personal Data Protection Law on 1 November 2021. Nor did the analysis identify the consequences of the divergence in equivalence in respect of the Data Transfers. As a result, TikTok Ireland's assessments did not demonstrate how these divergences interact with the specific transfers under consideration in the Inquiry and how the Problematic Laws interact with personal data that is processed in China by means of the Remote Access Solution.

399. By failing to adequately define the scope of the divergences, TikTok Ireland failed address how those divergences could impact EEA User Data that is processed in China. As a result, TikTok Ireland failed to

[174] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 218.
[175] The Assessment dated 13 October 2022 in respect of the position under the 2010 SCCs, and the Data Transfer Assessments dated 19 December 2022 and October 2023 in respect of the position under the 2021 SCCs, TikTok Ireland.

adequately assess the law and practices in effect in China in the context of the Data Transfers and the level of protection that is provided to the personal data of EEA Users.

400. TikTok Ireland's response to the Preliminary Draft Decision disputed that its Data Transfer Assessments failed to adequately assess these matters. In its submissions in response to the Preliminary Draft Decision, TikTok Ireland submitted that its assessments considered each of the four Essential Guarantees set out in the Essential Guarantees Recommendations in Sections 2.1 to 2.4, and, at Section 2.5, the international treaties and similar agreements that China is a party to.[176] TikTok Ireland's submissions in response to the Preliminary Draft Decision also mapped where it considered each Essential Guarantee was considered in its 2021 and 2022 Data Transfer Assessments. Those submissions also provided what TikTok described as *"additional information regarding the divergences and resulting risks"*, and the submissions responded to the DPC's assessment in the Preliminary Draft Decision. The DPC has had regard to all of this information for the purposes of this Decision.

401. TikTok Ireland's response to the Preliminary Draft Decision summarised how its Data Transfer Assessments identified gaps with the requirements of Essential Guarantee A as follows:

> 1) Certain laws lack a clear definition of the scope of the limitation on the exercise of the right concerned, in what circumstances and under which conditions the measure may be adopted or the minimum safeguards to the extent required by the EU standard. These laws were identified as Article 38 of the Counter-Espionage Law, Article 20 of the Counter-Espionage Law, and Article 28 of the Cybersecurity Law.
>
> 2) The specific criteria for granting approval to a Chinese authority exercising its powers under the laws described in Section 2.2 tend not to be published.
>
> 3) Whilst the Criminal Law sets out quite detailed rules regarding the use of technical investigative measures, they are not as clear and precise when it comes to requests for disclosure of data other than pursuant to technical investigative measures.
>
> 4) The full effect of the Personal Information Protection Law as a matter of practice is not yet fully established.[177]

402. TikTok Ireland's response to the Preliminary Draft Decision summarised how its Data Transfer Assessments identified gaps with the requirements of Essential Guarantee B as follows:

> 1) It is unclear in practice how the technical investigative measures under Article 150 of the Criminal Procedure Law are applied to the principle of necessity and proportionality.
>
> 2) The scope of the terms *"organisation and/or citizen",* "*support, assist and cooperate*" are not clearly defined under the National Intelligence Law. As a result, it is not possible to determine whether in all circumstances a request would be necessary and proportionate as the duty to "support, assist and cooperate" does not seem otherwise qualified. For example, there are no factors detailing what

[176] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at Paragraphs 2 and 3 to Schedule B.
[177] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at Paragraphs 20 to Schedule B.

actions organisation or individual can be expected and what factors would necessitate more or less interference with the right to privacy of an individual where a request for access to data was made.

3) The requirement for organisations to "*facilitate and provide other assistance*" in counter-espionage efforts is not clearly defined in the Counter-Espionage Law. Therefore, the scope of the application is unclear. As a result of the unclear definition, it is not possible to determine whether in all circumstances a request would be necessary and proportionate as the duty to "facilitate and provide other assistance" does not seem otherwise qualified as there are no factors to take into account.

4) Article 18 of the Anti-Terrorism Law requires internet service providers to provide technical interfaces, decryption and other technical support to prevent terrorist activities in accordance with the law. This gives rise to the concern that encrypted data in China could be decrypted and thus not be subject to the same protections as in the EU. This is due to internet service providers not having a clear obligation which could lead to disproportionate and unnecessary action being taken.

5) The obligation on network operators to provide "*technical support and assistance*" to the public security bureau and the national security bureau for national security or criminal investigation is not clearly defined. This could lead to different interpretations being taken in practice and, in turn, the principles of proportionality and necessity not being applied.[178]

403. TikTok Ireland's response to the Preliminary Draft Decision summarised how its Data Transfer Assessments identified gaps with the requirements of Essential Guarantee C as follows:

1) The Data Transfer Assessment stated: "...regulatory authorities may not be as independent of government as certain regulatory authorities in the EU." This is due to the fact that they are still part of the executive and conduct oversight on the upper levels of the same branch. The Data Transfer Assessment clarifies that the laws require these agencies to be independent in any event: "The National Supervisory Commission is mandated by the PRC Constitution and the National Supervisory Law to exercise its supervisory power independently and free from interference by any administrative authority, social organisation or individuals.The National Supervisory Commission and local supervisory commissions are elected by the Peoples' Congress and they are only accountable to the Peoples' Congress and the Standing Committee of the People's Congress…The People's Procuratorates are required by the PRC Constitution to exercise their legal supervisory power independently and free from interference by any administrative authority, social organisation and individual."

2) The Data Transfer Assessment notes: "As stated above, the Cyberspace Administration of China and sectoral regulators do not have oversight of national security agencies from a data protection perspective. The lack of oversight of national security agencies from a data protection perspective is similar to the position in the EU, given the carve out for national security activities in the GDPR. There is independent oversight of these agencies with respect to surveillance in any event as review of surveillance measures can occur by way of internal oversight (i.e. pre-approval of surveillance measures) as discussed in (1) above under the heading "Internal oversight" and judicial oversight (as

[178] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at Paragraphs 52 to Schedule B.

discussed in Section 2.4) and by way of the National Supervisory Commission (as discussed in this Section 2.3) and the People's Procuratorates (as discussed in this Section 2.3 and Section 2.4)."

3) There is no prior judicial authorisation over surveillance measures: "...whilst the laws set out in Section 2.2 include various requirements for prior approval before a Chinese authority can obtain data in accordance with the powers granted under those laws, there is no mechanism for prior review and approval by a judge or other independent body outside the Chinese authority (e.g. an administrative body or parliamentary body) whose decision is binding and is as independent of government as required by the EU standard…".

4) As noted in the Data Transfer Assessment, "the rules and criteria for internal approval tend not to be published". Therefore, it is not possible for the Chinese authorities to be open to public scrutiny to the extent required by Essential Guarantee C.[179]

404. TikTok Ireland's response to the Preliminary Draft Decision summarised how its Data Transfer Assessments identified gaps with the requirements of Essential Guarantee D as follows:

> 1) A data subject will not be notified in all the circumstances in which surveillance measures take place. The Data Transfer Assessment stated: "Chinese authorities are permitted by law to impose confidentiality obligations in the process of investigation or law enforcement and there is no specific obligation under Chinese law to inform a data subject once surveillance is over. As a result, a person may not be informed that a Chinese authority has obtained their data in certain cases. This could impact on their ability to exercise their rights, including their rights of redress. However, if information gathered from the use of technical investigative measures were used in criminal proceedings against an individual (such as a national security related crime for breach of the Anti-Terrorism Law or Counter-Espionage Law), they would be made aware as this would form part of the case file against the individual….Whilst these provide some mitigations and individuals are able to understand where information obtained through technical investigative measures or otherwise will be used in criminal proceedings, it remains possible that in at least certain cases an individual may not be informed that their data has been obtained by a Chinese authority. Consequently, whilst Chinese law provides a high level of safeguards regarding the right of redress, it diverges in this respect from what is required by the EU standard."[180]

405. Therefore, TikTok Ireland's position is that its assessment of Chinese law and practices adequately identified and articulated the manner in which Chinese law diverges from EU law.

406. Analysis of these submissions of TikTok Ireland points to a lack of specific criteria or detailed rules governing how Chinese authorities exercise their powers under the aforementioned problematic laws. TikTok Ireland cited confidentiality obligations and circumstances where individuals may not be informed that their data has been obtained by a Chinese public authority including where a state secret, national intelligence, or co-operation with criminal investigative measures imposed by a public authority is at issue.

---

[179] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at Paragraphs 62 to Schedule B.

[180] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at Paragraphs 75 to Schedule B.

407. TikTok Ireland contends that its assessment of Chinese law and practices nonetheless adequately identified and articulated the manner in which Chinese law diverges from EU law. In this regard, in response to the Preliminary Draft Decision, TikTok Ireland submitted:

> The DPC's assertion that the Data Transfer Assessment does not adequately identify the manner in which Chinese law diverges from EU law in respect of data protection or the reasons for the lack of essential equivalence (which arises when SCCs alone are used) is incorrect. TikTok adequately assessed the Chinese legal framework against each of the Essential Guarantees set out in the Essential Guarantees Recommendations. To further illustrate this to the DPC, TikTok has mapped in Schedule B where specifically the Data Transfer Assessment identified the manner in which Chinese law diverges from the Essential Guarantees (which arises when SCCs alone are used).
>
> In Section 2 of the Data Transfer Assessment, TikTok concluded that Chinese law is not essentially equivalent to what is required by the EU standard where SCCs alone are used (i.e. without consideration of the specific circumstances of the Data Transfers), due to the divergences from the Essential Guarantees. As demonstrated in Schedule B at paragraph 19, the Data Transfer Assessment identifies and explains why TikTok reached this conclusion. This assessment in Section 2 of the Data Transfer Assessment involved a detailed analysis of each of the Chinese laws that were of potential relevance in assessing divergences from the Essential Guarantees (such as the Anti-Terrorism Law, Counter-Espionage Law, and Criminal Law). Based upon this detailed analysis, TikTok identified the key reasons for concluding that there was no essential equivalence where SCCs alone are used for transfers.
>
> Importantly, TikTok also concluded in Section 2 that this did not apply to data stored outside China that could be remotely accessed in China, i.e. the divergences were not problematic for such data (or, in other words, did not result in a lack of essential equivalence for such data). TikTok assessed in Section 3 of the Data Transfer Assessment whether the divergences from the Essential Guarantees were relevant to the Data Transfers in the specific circumstances, including having regard to the supplementary measures in place. TikTok concluded, for the reasons already outlined in Section VI, Part D above, that the divergences were not relevant to the remotely accessible EEA User Data as it is stored outside China and that, consequently, there were no resulting risks to EEA Users and that there was an essentially equivalent level of protection.
>
> TikTok's assessment accords with the steps for a data transfer assessment set out in the Supplementary Measures Recommendations, and the Essential Guarantees Recommendations.
>
> Without prejudice to TikTok's position that it did adequately assess the potential divergences from the Essential Guarantees (and potential resulting risks), as the divergences identified in Section 2 of the Data Transfer Assessment when SCCs alone are used are not relevant or applicable with respect to the remotely accessible EEA User Data, TikTok was not required to provide further analysis or detail on the scope of the potential divergences between Chinese law and the Essential Guarantees in the Data Transfer Assessment.
>
> Moreover, insofar as the DPC in the PDD is suggesting that the Data Transfer Assessment should have identified at a more granular level the divergences between the level of protection under the Chinese legal framework and the Essential Guarantees or set out the resulting risk to the protection of data subjects' personal data, this is not required by the GDPR, the SCCs, the Essential Guarantees Recommendations or the Supplementary Measures Recommendations. Further, the DPC does not point to any authority for this proposition.

The DPC's provisional conclusions appear to be based on the incorrect premise that it was incumbent on TikTok to identify all divergences between EU and Chinese law and to assess the risks arising from these divergences. This is not consistent with the judgment of the CJEU in Schrems II, which makes clear that the obligation on TikTok was to assess, as regards any potential access by the public authorities of China to the remotely accessed EEA User Data, the relevant aspects of the legal system of China. Further, in doing so, TikTok correctly had regard to the circumstances of the Data Transfers, consistent with Schrems II.

For the reasons set out above, TikTok submits that it adequately assessed Chinese law and practice against the Essential Guarantees, including by analysing and identifying any potential divergences and resulting risks to the extent required to properly undertake a data transfer assessment. TikTok accordingly requests that the DPC reconsider its provisional view that it failed to do so.[181]

408. The DPC does not accept TikTok Ireland's submissions in this regard for a number of reasons. First, the findings in this Decision are not based on the premise that it was incumbent on TikTok to identify all divergences between EU and Chinese law and to assess the risks arising from these divergences. Rather, regarding TikTok Ireland's obligation to assess the law and practices in effect in China in the context of the Data Transfers, there was an obligation on TikTok Ireland to assess the divergences as they apply in the specific context of the transfers. TikTok Ireland has clearly failed to do this. TikTok Ireland has not verified or guaranteed the basis for its position that the divergences were not of relevance to the Data Transfers in their specific circumstances because TikTok Ireland failed to consider how the divergences interact with the EEA User Data that was processed on computer information systems in China.

409. Second, the DPC does not accept TikTok Ireland's submission that it adequately assessed the Chinese legal framework against each of the Essential Guarantees set out in the Essential Guarantees Recommendations. The DPC acknowledges that TikTok Ireland set out the basis for its conclusions that there are aspects of the Chinese legal framework that preclude a finding of essential equivalence to EU law, even where SCCs are used. However, when setting out the divergences that TikTok Ireland acknowledged to exist, TikTok Ireland did so in general terms only and did not provide sufficient information to enable a consideration of the specifics regarding how those divergences could apply to EEA User Data subject to the Data Transfers. When setting out the divergences, TikTok Ireland also failed to consider the extent of the resulting risk to the protection of personal data of EEA Users. In setting out the divergences, TikTok Ireland did not adequately define the scope of the divergences and simply set them out in high level terms without considering how they could apply to EEA User Data subject to the Data Transfers.

410. For example, the Data Transfer Assessments acknowledged that there are obligations on organisations and citizens in China to support, assist and cooperate with state intelligence work. However, TikTok Ireland did not consider to what extent this support, assistance and cooperation could apply to those computer information systems in China, including devices of the employees of the China Group Entities. TikTok Ireland did not address whether such support, assistance and cooperation could extend to citizens in China who are employees of the China Group Entities and whether those employees could assist state intelligence work by supporting direct or indirect access to those computer information systems. TikTok Ireland's position also

[181] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at Paragraphs 243 – 251.

does not address whether access by Chinese authorities to those computer information systems could lawfully occur without the knowledge of the China Group Entities and/or their employees. Neither does it address the modalities of any such requests by Chinese authorities and whether any such access could be by manual or by other means.

411. TikTok Ireland's Data Transfer Assessments also acknowledged that Chinese authorities are permitted by law to impose confidentiality obligations in the process of investigation or law enforcement and there is no specific obligation under Chinese law to inform a data subject once surveillance is over.[182] TikTok Ireland acknowledged that it is possible that an individual may not be informed that their data has been obtained by a Chinese authority and, consequently, that Chinese law diverges in this respect from what is required by the EU standard. However, TikTok Ireland's analysis failed to define the scope of this divergence and failed to consider how it could impact EEA User Data that is processed in China.

412. In addition to these examples, TikTok Ireland's Data Transfer Assessments show, across the multiple additional distinct divergences between the Chinese legal framework and EU standards, that Chinese Authorities have broad surveillance powers. TikTok Ireland's assessments set out vague, undefined investigative and surveillance powers that exist under Chinese law and practices. In this context, TikTok Ireland chose not to address the issue of EEA User Data in China but rather focused on Chinese law and practices as they pertain to EEA User Data located outside China. In identifying each of these divergences, TikTok Ireland failed in each case to sufficiently set out the scope of the divergences, which resulted in insufficient information to consider how those divergences might apply to EEA User Data subject to the Data Transfers. Rather, in each case, TikTok Ireland relied on the territoriality principle for the proposition that EEA User Data is beyond the reach of Chinese Authorities.

413. The DPC does not accept the basis for TikTok Ireland's conclusion that the key reasons that it had identified for concluding that there was no essential equivalence where SCCs alone are used did not apply to personal data transferred to China by means of remote access. TikTok Ireland's failure to set out in a clear way the deficiencies it acknowledged to exist in the Chinese legal framework is particularly problematic in light of the difficulties identified above with TikTok Ireland's assessment of the territoriality principle. Having acknowledged that divergences exist, the Data Transfer Assessments concluded that those divergences do not result in a lack of essentially equivalent protection in respect of transfers made by way of remote access on the basis of TikTok Ireland's assessment of the territoriality principle. TikTok Ireland's failure to consider how the territoriality principle applies in respect of the personal data that is processed by TikTok Ireland in China undermines its conclusion that the divergences did not result in a lack of essentially equivalent protection based on the application of the territoriality principle. Its failure to identify with sufficient clarity the extent of the risk to data subjects resulting from the material divergence subsequently impacts it ability to choose supplementary measures. The DPC has carefully considered all of the information submitted by TikTok Ireland during the Inquiry, having particular regard to Sections 2 and 3 of the Data Transfer Assessments. The DPC finds that TikTok Ireland failed to both adequately define the scope of those divergences from EU standards as they apply to the Data Transfers, and to address the extent of the resulting risk to the protection of personal data of EEA users.

414. This failure has very significant consequences for the Data Transfer Assessments. TikTok Ireland's failure to identify these divergences with sufficient clarity means that the Assessments provide insufficient information to consider how those divergences might apply to EEA User Data subject to the Data Transfers. The Assessments do not account for the possibility of public authority surveillance in respect of the EEA User Data

[182] Data Transfer assessment dated 19 December 2022 at page 54.

that is processed in China pursuant to the Remote Access Solution. For example, in light of this failure, it is not possible to assess: the scope of potential access to that data by public authorities in China, and the powers that may be available to the public authorities in that respect; the obligations on the China Group Entities or their employees to assist public authorities accessing data as it is processed in China; the extent to which such access could occur with or without the knowledge of TikTok Ireland and/or the China Group Entities and/or the employees of the China Group Entities; and the capacity for public authorities to directly or indirectly obtain access to EEA User Data as it is processed on computer information systems in China with or without the assistance of employees of the China Group Entities.

415. By failing to consider the divergences as they apply to the Data Transfers, TikTok Ireland failed to establish a number of crucial issues in respect of the level of protection afforded to the personal data transferred by means of the Remote Access Solution. It is not clear which surveillance measures risk being applied to computer information systems in China that process EEA User Data. It is not clear to what extent such measures could be applied with or without the assistance and/or knowledge of the China Group Entities and/or their employees. In addition to the lack of information regarding the risk of individuals providing the Chinese authorities with EEA User Data after it has been routinely transferred to China, there is also a lack of information regarding the extent of the risk that such information could be directly obtained by Chinese authorities from computer information systems in China, either with or without the assistance of employees of the China Group Entities. Furthermore, there is a lack of information regarding confidentiality obligations that might apply to the China Group Entities and/or their employees in respect of surveillance measures.

416. In light of TikTok Ireland's ongoing failure to appropriately consider how the territoriality principle applies in respect of the Data Transfers, and its ongoing failure to adequately set out the deficiencies that it acknowledges to exist in the Chinese legal framework, the DPC finds that TikTok Ireland has, on a continuing basis, failed to adequately assess the level of protection provided to EEA User Data by Chinese law and practice in the context of the transfers using SCCs.

e) DPC Findings in respect of Issue 2

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 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 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.

419. To verify that EEA User Data would be subject to an essentially equivalent level of protection, TikTok Ireland was first required to comprehensively assess the law and practices in China in the context of the Data Transfers using SCCs. Its failure to do so rendered any apparent verification of essential equivalence invalid because, in order to verify essential equivalence, it is necessary to substantiate all relevant aspects of the law and practices that could have a bearing on that level of protection provided to the specific Data Transfers. Having assessed the law of the third country, in order to verify and guarantee an essentially equivalent level of protection, the controller or processor must assess whether the appropriate safeguards, enforceable rights and effective legal remedies ensure that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the European Union. This requires an assessment of the appropriate safeguards and supplementary measures in light of the proposed transfers and the law of the third country.

420. It is clear that the application of the territoriality principle to the specific transfers under consideration in this inquiry, which involves the Remote Access Solution, and therefore the inevitable processing of personal data on computer information systems located in China, is an issue of considerable importance to the question of essential equivalence. This is because the territoriality principle is crucial to the question of the application of problematic laws to EEA User Data as it is processed in China. By failing to adequately assess the law and practices in China in this respect, TikTok Ireland failed to verify that EEA User Data would be subject to an essentially equivalent level of protection.

421. To guarantee that EEA User Data would be subject to an essentially equivalent level of protection, TikTok Ireland was also first required to comprehensively assess the law and practices in China in the context of the Data Transfers using SCCs. Article 46 GDPR enables transfers of personal data to a third country to occur in the absence of an adequacy decision only if the controller or processor has provided appropriate safeguards. The purpose of appropriate safeguards and supplementary measures is to compensate for deficiencies in the protection afforded by the third country. In order to compensate for those deficiencies, it is imperative to first identify the deficiencies with sufficient clarity by assessing the law and practices of the third country in the context of the Data Transfers.

422. TikTok Ireland's failure to adequately assess the level of protection provided by Chinese law and practice prevented it from guaranteeing that the law and practices in China did not undermine the effectiveness of the SCCs, and the supplementary measures as set out in Issue 3, in ensuring an essentially equivalent level of protection. SCCs are contractual in nature and cannot compensate for certain inadequacies in the legal framework of third countries, particularly inadequacies relating to access to personal data by surveillance authorities. The legal context in a third country can make the obligations set out in the SCCs impossible to implement. For example, as acknowledged in the Schrems II judgment, compliance with an obligation prescribed by the law of a third country which goes beyond what is necessary in a democratic society to safeguard inter alia, national security, defence and public security must be treated as a breach of the SCCs. TikTok Ireland's assessment of Chinese law and practices acknowledged that it does not provide an essentially equivalent level of protection to that provided in the European Union. However, its position that the divergences identified in Sections 2.1 – 2.5 of the Data Transfer Assessments do not undermine the safeguards provided on the basis of the territoriality principle, was not established. The DPC finds that TikTok Ireland failed to verify, guarantee and demonstrate that the divergences identified do not undermine the effectiveness of the SCCs, and, accordingly, it failed to verify, guarantee and demonstrate that data subjects have enforceable rights and effective legal remedies.

423. In order to compensate for deficiencies, and guarantee same, it is crucial to know what those deficiencies are. Only following an assessment of the law and practices of the third country is it possible for the controller or processor to determine whether, having regard to appropriate safeguards and supplementary measures, the transfer can operate based on a level of protection essentially equivalent to that which is guaranteed within the European Union. TikTok Ireland's failure to assess, in light of the Data Transfers, the deficiencies in the protection afforded in China meant that it was not in a position to select appropriate safeguards and supplementary measures that guarantee an essentially equivalent level of protection, and that guarantee that data subjects have enforceable rights and effective legal remedies. The DPC notes in particular that SCCs are inherently contractual in nature and cannot bind the public authorities of third countries. Therefore, in order to guarantee an essentially equivalent level of protection in light of SCCs, it is necessary to base any such guarantee on a comprehensive assessment of the law and practices of the third country. TikTok Ireland has failed to do so and accordingly has failed to guarantee 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.

424. Therefore, the DPC finds that TikTok Ireland's failure to establish how the territoriality principle applies in the specific context of the Data Transfers and its failure to establish the extent of the deficiencies it acknowledged to exist in the Chinese legal framework has prevented it from verifying and guaranteeing that an essentially equivalent level of protection is provided in light of safeguards implemented. This has prevented TikTok Ireland from verifying and guaranteeing that data subjects have enforceable rights and effective legal remedies. Having failed to verify and guarantee that the Data Transfers were afforded a level of protection essentially equivalent to that guaranteed within the European Union, it is clear that TikTok Ireland was also not in a position to demonstrate an essentially equivalent level of protection.

G. Issue 3 - Supplementary Measures

425. As set out above TikTok Ireland determined that, in the specific context of the Data Transfers, and in light of its assessment of China's legal framework in Section 2 of the 2021 and 2022 Data Transfer Assessments, the 2010 SCCs and the 2021 SCCs should be reinforced by supplementary measures.

426. In the Data Transfer Assessments from 2021 and 2022, TikTok Ireland described the Supplementary Measures outlined in Section 3 of those Assessments as providing for the transfers to be implemented by way of secure Remote Authorised Access, ensuring the effectiveness of the SCCs, and affording EEA User Data a level of protection essentially equivalent to that guaranteed within the European Union. Those assessments did not make any reference to the storage of EEA User Data on servers in China that TikTok Ireland notified the DPC of in April 2025, but which was ongoing during the temporal scope.

427. The DPC has set out under Issue 2 above how TikTok Ireland's 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 to the China Group Entities using SCCs 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. For the reasons that follow, the supplementary measures implemented by TikTok Ireland do not rectify this failure and TikTok Ireland has failed to verify, guarantee and demonstrate that the supplementary measures ensure that EEA Users are provided with the appropriate safeguards, enforceable rights and effective legal remedies so that the personal data of EEA Users is afforded a level of protection essentially equivalent to that guaranteed within EU.

a) Supplementary measures in the context of Articles 44 and 46 GDPR

428. Guidance relating to the manner in which supplementary measures should be evaluated is found in both the Schrems II judgment, and in the EDPB Supplementary Measures Recommendations. The Schrems II judgment reflected how SCCs, as envisaged by Article 46(2) GDPR, may comprise a particular form of *"appropriate safeguards"* for the purpose of data transfers to third countries.

429. However, as the CJEU found, while SCCs are binding on a controller established in the EU and the transfer recipient in the third country, *"those clauses are not capable of binding the authorities of that third country, since they are not party to the contract".*[183]

430. Consequently, while there are situations in which, depending on the law and practices in force in the third country concerned, the transfer recipient is in a position to guarantee the necessary protection of the data solely on the basis of SCCs, there are others in which the content of the SCCs may not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned.[184]

431. Critically, in this respect, the CJEU held that:

---

[183] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 125.
[184] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 126.

> That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.[185]

432. Therefore, if SCCs fail to provide the required level of protection and to compensate for any lack of data protection in the third country, it will be necessary to consider whether there are any supplementary measures in place which could compensate for inadequate protection in the third country. In order to compensate for any lack of protection by means of supplementary measures, it is imperative to first identify the existing deficiencies with sufficient clarity by assessing the law and practices of the third country in the context of the Data Transfers. The DPC has set out at Issue 2 above how TikTok Ireland failed to do so.

433. In this regard, the CJEU envisaged that *"[…] it may prove necessary to supplement the guarantees contained in [the] standard data protection clauses"* by providing *"other clauses of additional safeguards"* to *"supplement"* the SCCs.[186]

434. Moreover, *"depending on the prevailing position in a particular third country"*, supplementary measures may need to be adopted by the controller to ensure compliance with the level of protection available within the EU.[187]

435. Supplementary measures must, in light of recital 108 GDPR, compensate for the lack of data protection in a third country in order to ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union. The supplementary measures must not merely mitigate, minimise or reduce the deficiencies in the law of the third country, but rather must ensure that data subjects receive essentially equivalent protection to EU law.

436. Thus, the controller or processor must:

> […] verify, on a case-by-case basis and, where appropriate, in collaboration with the [importer] whether the law of the third country … ensures adequate protection, under EU law … by providing, where necessary, additional safeguards to those offered by [the 2010 SCCs].[188]

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

438. The CJEU added that:

> 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,

---

[185] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 126.
[186] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 132.
[187] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 133.
[188] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 134.

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.[189]

439. As set out above, the controller or processor, in addition to verifying and guaranteeing the adequacy of protection, must be able to demonstrate that adequacy in practice.

440. The Supplementary Measures Recommendations give the following further assistance with the assessment of the adequacy of measures supplementary to SCCs:

(i) "*Supplementary measures"* are by definition supplementary to the safeguards the Article 46 GDPR transfer tool already provides and to any other applicable security requirements (e.g. technical security measures) established in the GDPR.[190]

(ii) Supplementary measures should "*prevent the risk of potential application to [the data importer] importer and/or to [the] transferred data of laws and/or practices of the third country of the data importer"*.[191]

(iii) Supplementary measures may have a contractual, technical or organisational nature. Combining diverse measures in a way that they support and build on each other may enhance the level of protection and may therefore contribute to reaching EU standards. However, contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices, and there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data.[192]

441. In Section 3 of each of the 2021 and 2022 Data Transfer Assessments, TikTok Ireland described the supplementary measures under the following headings, each of which is considered in turn below:

(i) Technical Measures,

(ii) Contractual Measures,

(iii) Organisational Measures.

[189] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), at paragraph 135.
[190] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021), at page 21.
[191] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021), at pages 17–18.
[192] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021), at page 22.

b) Technical measures

442. TikTok Ireland outlined its technical measures in Section 3.1 of its 2021 and 2022 Data Transfer Assessments both in general overview and provided the Inquiry further details of specific technical measures it applies, as outlined below.

i. System entry controls

443. TikTok Ireland indicated that the following system entry controls applied to the systems relevant to the remote access to EEA User Data the subject of the transfers:[193]

[redacted]

444. [redacted]

ii. Encryption

445. TikTok Ireland outlined how it applied encryption to protect the personal data of EEA users the subject of the transfers.

---

[193] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 28-29, Data Transfer Assessment – China Group Entities dated 13 October 2022, at pages 57-58 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 72–73.
[194] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at page 36.

446. It stated that:

(i) EEA user data in transit was encrypted using [redacted] with [redacted] For internal access to systems, including web access and server access, [redacted] For remote access to IT systems within the network, [redacted] were used to protect against external threats.

(ii) EEA user data, [redacted] were used to encrypt certain data elements, including certain basic user information (i.e. name, birth date, gender, phone number, and email address), user account passwords, certain user interaction/activity, device information, direct messages, and private videos.[195]

447. TikTok Ireland confirmed that the format of the personal data the subject of remote access by the China Group Entities was '*Encrypted / Pseudonymised / Plain-text*'. As outlined under Issue 1, personnel of the China Group Entities were granted authorisation, based upon the role or function they perform, and the existence of a legitimate business need, for access to data in decrypted or plaintext form. The approval process for requests for access to decrypted or plaintext personal data of EEA Users was regulated in accordance with TikTok's general access permission processes and is subject to the same oversight.[196]

448. TikTok Ireland stated that:

> [b]ased on demonstrated need (such as the investigation of security incidents), authorised personnel within China Group Entities can request the ability to see decrypted data elements. [redacted]

449. [redacted]

450. [redacted]

[195] For example, page 29 of Data Transfer Assessment – China Group Entities dated 12 October 2021.
[196] TikTok Ireland's Response dated 20 June 2022, at page 15.
[197] Data Transfer Assessment – China Group Entities dated 12 October 2021, at page 29, Data Transfer Assessment – China Group Entities dated 13 October 2022, at page 58 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at page 73.

[redacted]

451. [redacted]

452. When reviewing TikTok Ireland's submissions in this regard, the DPC has taken note of Use Cases 6 and 7 in Annex 3 to the EDPB Supplementary Measures Recommendations.

453. Use Case 6 is as follows:

> Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear
>
> 94. A data exporter transfers personal data, whether by electronic transmission or by making it available to a cloud service provider or other processor to have personal data processed according to its instructions in a third country (e.g., for the provision of technical support or any type of cloud processing), and this data is not - or cannot- be pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear.
>
> If
>
> 1. a controller transfers personal data to a cloud service provider or other processor,
>
> 2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
>
> 3. the power granted to public authorities of the recipient country to access the transferred data in question goes beyond what is necessary and proportionate in a democratic society, where in practice problematic legislation of the third country applies to the transfers in question,
>
> then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on the data subject's fundamental rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.
>
> 95. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

454. Use Case 7 is similar, as follows:

> Use Case 7: Transfer of personal data for business purposes including by way of remote access
>
> 96. A data exporter transfers personal data to entities - in a third country to be used for shared business purposes —whether by electronic transmission or by making it available to remote access by

[198] TikTok Ireland's Response dated 12 October 2021, Schedule, Document 9.

the data importer—, and this data is not - or cannot- be -pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear. One typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.

If

1. a data exporter transfers personal data to a data importer in a third country by making it available in an information system in a way that allows the importer direct access to data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,

2. the importer processes the data in the clear in the third country (including for its own purposes where the importer is a controller),

3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society, where in practice problematic legislation of the third country applies to the transfers in question (see Step 3),

then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on the data subject's fundamental rights.

97. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

455. In respect of the key features of the scenarios outlined in Use Cases 6 and 7 above, the DPC notes that:

(i) There were transfers by a controller, TikTok Ireland, to processers and sub-processors in China, the China Group Entities.

(ii) There were situations in which the China Group Entities needed access to the personal data of EEA users in the clear, that is in plaintext or decrypted form, in order to execute the tasks assigned to them.

(iii) TikTok Ireland, as outlined under Issue 2 above, identified a number of respects in which the law and practices in effect in China, in particular with regard to the investigative and surveillance powers granted to public authorities in China, do not comply with the Essential Guarantees Recommendations. There is a risk that problematic laws may potentially apply to the Data Transfers in circumstances where TikTok Ireland's assessment did not contain clarity concerning the application (or indeed relevance) of the territoriality principle in connection with those laws in the specific context of the remote access by which the transfers are effected. In particular, the Data Transfer Assessments failed to address the application of the territoriality principle in the specific factual context of the EEA User Data that was transferred to China and processed there.

(iv) TikTok Ireland disputes that problematic laws apply in practice to the personal data the subject of the Data Transfers made by means of the Remote Access Solution. However, as set out under Issue

2, TikTok Ireland failed to establish that the territoriality principle prevents the application of problematic laws to EEA User Data when that personal data is processed in China. Therefore, there is an unassessed risk that problematic laws may apply to the transfers. Any supplementary measures implemented must be effective to prevent that risk. However, in order to verify, guarantee and demonstrate an essentially equivalent level of protection in light of the supplementary measures implemented, it was an essential prerequisite that TikTok Ireland first identify the existing deficiencies with sufficient clarity by assessing the law and practices of the third country in the context of the Data Transfers. The DPC has set out at issue 2 above how TikTok Ireland failed to do so.

iii. Access Controls

456. TikTok Ireland explained the manner in which remote access to EEA User Data by China Group Entities was subject to data access controls, including a layered approval process and permissions based on a *"least privilege"* basis, with logging mechanisms to authenticate data access.

457. In this regard, TikTok Ireland explained that TikTok's data access approval process governed the process of granting data access permissions to any internal TikTok group personnel, including those in the China Group Entities. Authorised Access permissions were granted on a case-by-case basis and based on a demonstrated need. TikTok's data was divided into different levels of confidentiality according to the degree of sensitivity; the higher the level of confidentiality, the stricter the approval process. [redacted]

458. TikTok Ireland provided the following policy documents which record and document the data approval process outlined above both with regard to the position under the 2010 SCCs, and the updated position under the 2021 SCCs during the temporal scope:

Document	Date
[redacted]	
[redacted]	
[redacted]	
[redacted]	

459. [redacted]

[199] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 1.
[200] TikTok Ireland's Response dated 12 October 2021, Schedule, Document 8.
[201] TikTok Ireland's Response dated 28 March 2023, Schedule, Document 1.
[202] TikTok Ireland's Response dated 12 October 2021, Appendix A, Document 7.

[redacted]

460. [redacted]

iv. Network security and other measures

461. TikTok Ireland also relied on further network security and other measures during the temporal scope.

462. TikTok Ireland outlined that TikTok Ireland, TikTok UK, TikTok Pte. Limited, which owns and operates servers in Singapore, and TikTok, Inc., which owns and operates servers in the US, each holds ISO 27001 certification.

463. Copies of ISO certificates were provided for TikTok Technology Limited, TikTok Information Technologies UK Limited, TikTok Pte. Limited and TikTok Inc.[203] No relevant certifications were provided for the China Group Entities.

464. TikTok Ireland also referred to the information security certifications obtained by its third party vendors, in particular:

(i) [redacted] which it states holds the following certifications: BSI C5, ISO/IEC 27701, ISO/IEC 27018, ISO/IEC 27001, ISO/IEC 27017, SOC1, SOC2, SOC3; and

(ii) [redacted] which it states holds the following certifications: ISO/IEC 27001, ISO/IEC27701, and ISO27018, SOC1, SOC2 and SOC3.

465. [redacted]

[203] TikTok Ireland's Response dated 12 October 2021, Schedule, Document 11A, 11B, 11C, and 11D.

[redacted]

c) Contractual measures

466. The contractual measures that TikTok Ireland outlined are set out below.

i. The 2020 Intra-Group Agreement relating to the 2010 SCCs

467. [redacted]

468. TikTok Ireland's position is that while the 2010 SCCs alone would not provide a level of protection essentially equivalent to that provided under EU law in light of the deficiencies identified in Chinese law, the additional contractual measures it had in place were effective, when taken together with the technical and organisational measures it had implemented, to provide such protection.

469. TikTok Ireland referred at section 3.2 of its Data Transfer Assessments, in particular to:[204]

(i) [redacted] of the 2020 Intra-Group Agreement, which stipulated that in the event of any conflict between the 2010 SCCs and any other contractual provision within the Intra-Group Agreement, that the SCCs would prevail, reinforcing Clause 10 of the 2010 SCCs, [redacted]

[redacted]

470. [redacted]

[204] Data Transfer Assessment dated 12 October 2021, at pages 34–36, Data Transfer Assessment dated 13 October 2022, at pages 63–64.
[205] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 2.

[redacted]

471. TikTok Ireland also referred to the contractual obligations on its external cloud providers, and contractual confidentiality obligations imposed on its employees.

ii. The 2022 Intra-Group Agreement relating to the 2021 SCCs

472. In respect of the contractual measures in effect following the entry into force of the 2022 Intra-Group Agreement, TikTok Ireland similarly referred to:[206]

[redacted]

473. TikTok Ireland also summarised its obligations relating to law enforcement requests [redacted]

[206] Data Transfer Assessment dated 19 December 2022, at pages 78–79.
[207] TikTok Ireland's Response dated 28 March 2023, Schedule, Document 4.

[redacted]

474. [redacted]

d) Organisational measures

i. Generally

475. The organisational measures TikTok Ireland relied on to complement the measures outlined above were outlined at Section 3.3 of the each of the 2021 and 2022 Data Transfer Assessments.[208]

[208] Data Transfer Assessment – China Group Entities dated 12 October 2021, at pages 37–42, Data Transfer Assessment – China Group Entities dated 13 October 2022, at pages 65–70 and Data Transfer Assessment – China Group Entities dated 19 December 2022, at pages 81–87.

476. [redacted]

Document	Date
[redacted]	[redacted]

477. [redacted]

478. TikTok Ireland also outlined its EEA Data Transfer Policy as approved and formally adopted by the European Data Protection Steering Committee on 15 March 2021 which was set out in the following document:

Document	Date
TikTok EEA Data Transfer Policy	15 March 2021[210]

479. An audit of a number of policies relevant to the transfers the subject of the Inquiry, including the Data Transfer Assessment for China then in effect, [redacted], with which [redacted], was carried out by TikTok's EMEA Internal Audit and Risk Control team under [redacted] and recorded in a document furnished by TikTok Ireland:

Document	Date
[redacted]	[redacted]

480. With regard to organisational measures on data sharing, [redacted] TikTok reiterated, as noted above, that it did not share EEA User Data with other ByteDance companies in China for use in other ByteDance products (including Toutiao and Douyin).

481. Organisational measures relating to review, governance, and oversight of TikTok Ireland operations and policies relevant to the transfers were also referred to.

[209] TikTok Ireland's Response dated 12 October 2021, Appendix A, Document 7.
[210] TikTok Ireland's Response dated 12 October 2021, Appendix A, Document 7.
[211] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 3.

ii. Organisational measures relating to law enforcement requests

482. TikTok Ireland outlined that it had a law enforcement response team (*"LERT"*) who reviewed and evaluated law enforcement and governmental requests. The role of LERT employees is to perform checks to ensure that law enforcement requests from public authorities in different jurisdictions satisfy the requirements of the relevant jurisdiction, and verifies that it complies with TikTok's internal policies and procedures.

483. TikTok Ireland outlined TikTok's activities, policies and measures relating to internal training on LERT procedures, and external engagement with national law enforcement authorities and international agencies such as Europol and Interpol on TikTok Ireland's LERT policies and procedures. It clarified that to date, TikTok's LERT team had not conducted any outreach with China-based law enforcement agencies or other governmental authorities, as the LERT team has not received any requests from China-based law enforcement agencies or other governmental authorities.

484. With regard to internal employee training, it provided a copy of a LERT Training Presentation to TikTok's China team.[212]

485. TikTok Ireland outlined, further, that it implemented transparency measures relating to law enforcement requests, including guidelines on its website for the law enforcement community explaining the processes to be followed in the event a request needs to be submitted, and referred the following documents in this regard:

Document	Date
TikTok Law Enforcement Guidelines and Frequently Asked Questions (published online)	19 April 2021[213]
TikTok Law Enforcement Guidelines and Frequently Asked Questions (published online)	24 May 2022[214]

486. It also referred in this regard to the Transparency Reports published at least bi-annually on its website.[215] Prior to issuing the Preliminary Draft Decision, the DPC reviewed the Transparency Reports for H1 2019, H2 2019, H1 2020, H2 2020, H1 2021, H2 2021, and H1 2022, and confirmed that these Transparency Reports did not refer to law enforcement requests received from China.

487. TikTok's [redacted] on law enforcement requests for user data from public authorities in China was also set out in detail in Section 3.3 of the Data Transfer Assessments. The framework was set out in the following documents, relating, respectively, to the position under the 2010 SCCs and the 2021 SCCs:

Document	Date
[redacted]	[redacted]
[redacted]	[redacted]

[212] TikTok Ireland's Response dated 12 October 2021, Schedule, Document 10.
[213] TikTok Ireland's Response dated 12 October 2021, Appendix A, Document 3.
[214] TikTok Ireland's Response dated 28 March 2023, Schedule, Document 3.
[215] https://www.tiktok.com/transparency/en/
[216] TikTok Ireland's Response dated 12 October 2021, Schedule, Document 2.
[217] TikTok Ireland's Response dated 28 March 2023, Schedule, Document 2.

488. Within that framework, TikTok Ireland implemented [redacted]

489. Under the 2021 SCCs, [redacted]

[redacted]

490. The protocol was set out, in the versions applying to both the 2010 SCCs and the 2021 SCCs respectively, in the following documents:

Document	Date
[redacted]	[redacted]
[redacted]	[redacted]

491. [redacted]

e) Findings in respect of Issue 3

492. Under Issue 3, the issue the DPC must determine is whether, arising from the above, TikTok Ireland verified and guaranteed, and 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 were effective, together with the 2010 SCCs and the 2021 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 were afforded a level of protection essentially equivalent to that guaranteed within the EU.

[218] TikTok Ireland's Response dated 12 October 2021, Schedule, Document 4.
[219] TikTok Ireland's Submissions dated 19 December 2022, Schedule, Document 3.

493. There was an obligation on TikTok Ireland prior to making the transfers to first verify and guarantee that the personal data transferred would be subject to an essentially equivalent level of protection. In addition to verifying and guaranteeing an essentially equivalent level of protection for the transferred personal data, there is an obligation on TikTok Ireland to be able to demonstrate that the transfers were in fact provided an adequate level of protection, further to its obligations under Article 46 GDPR, having regard to the obligations in Articles 5(2) and 24 GDPR, as set out above.

494. The DPC has set out under Issue 2 how TikTok Ireland's 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 not only directly impacted TikTok Ireland's ability to select appropriate safeguards and supplementary measures, but also prevented TikTok Ireland from verifying, guaranteeing and demonstrating an essentially equivalent level of protection. TikTok Ireland's failure to identify with clarity the deficiencies it acknowledged to exist in the Chinese legal framework prevented it from selecting and implementing appropriate safeguards and supplementary measures to compensate for those deficiencies. It is possible to compensate for deficiencies only if those deficiencies are clearly identified in the context of the Data Transfers. This failure directly impacted on TikTok Ireland's ability to select supplementary measures and its ability to verify, guarantee and demonstrate that the supplementary measures and the SCCs were effective in respect of potentially problematic laws.

495. Notwithstanding this finding, the DPC has carefully considered all supplementary measures implemented by TikTok Ireland, as described above. For the reasons set out below, the DPC finds that TikTok Ireland failed to verify, guarantee and demonstrate that the supplementary measures and the SCCs were effective to ensure that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within the EU.

496. The supplementary measures implemented did not address the issue of the risk of Chinese authorities accessing the personal data that was remotely accessed by employees of the China Group Entities during the temporal scope of the Inquiry. This access by employees of the China Group Entities was by means of the Remote Access Solution and resulted in plain text processing of EEA User Data on computer information systems in China (as well as in encrypted and pseudonymised form). While the supplementary measures implemented by TikTok Ireland were reflective of a general level of security to prevent unauthorised access to the personal data processed in China by means of the Remote Access Solution, the DPC finds that those measures cannot act to prevent access supported by problematic laws.

497. The System Entry Controls, Network Security Measures, and Access Controls while reflective of general security, cannot act to prevent access by Chinese authorities supported by problematic laws. The majority of these measures are typical of the type of appropriate technical security measures for the purpose of Article 32 GDPR that an organisation engaged in processing of personal data of the nature, scale and complexity that TikTok Ireland is engaged in, and, in that regard, the DPC does not consider that the supplementary measures are of significant weight for the purpose of Article 46 GDPR regarding potential public authority access under problematic laws in a third country. 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 by employees of the China Group Entities in plain text. TikTok Ireland has set out a broad range of purposes for which personal data was accessed remotely in plain text. TikTok Ireland also set out the broad nature of what this processing entailed. This Decision sets out how these transfers were systematic, repetitive, and continuous. The DPC finds that the encryption measures implemented did not compensate for the lack of essentially equivalent protection in light of the data that was 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 obtaining access to the personal data that was processed in China in plain text. This personal data risked falling subject to such access irrespective of whether it was originally encrypted. For

example, the access controls do not address the potential for Chinese authorities to impose obligations on the employees of the China Group Entities in respect of personal data accessed in plain text, including obligations to support, assist and cooperate with those authorities by supporting direct or indirect access to the computer information systems in China or to EEA User Data as it is processed in China. Therefore, these technical measures cannot render ineffective potential access by public authorities in China supported by problematic laws.

498. The contractual measures are merely contractual in nature and are not binding on public authorities in China. Therefore, they cannot compensate for potential access supported by problematic laws. 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 failed to assess how these aspects of Chinese law or practices affect the suitability of the contractual measures as supplementary measures in terms of compensating for the lack of essentially equivalent protection. The organisational measures also cannot compensate for potential access under problematic laws as these measures cannot overcome access to personal data by public authorities where that access is supported by problematic legislation.

499. TikTok Ireland's failure to adequately consider how the divergences that it acknowledged to exist in Chinese law could apply to EEA User Data subject to the Data Transfers is particularly problematic in light of the risk of Chinese authorities obtaining access to the personal data that was processed in plain text. As set out under Issue 2 above, as a result of this failure, it is not clear which surveillance measures risk being applied to EEA User Data in China, and which measures Chinese authorities could potentially adopt to obtain access to EEA User Data. There is a risk that problematic laws may potentially apply to the Data Transfers in circumstances where TikTok Ireland's assessment did not contain clarity concerning the application or relevance of the territoriality principle in connection with those laws in the specific context of the remote access by which the transfers are effected in China. The obligation rests with TikTok Ireland to verify, guarantee and demonstrate that any supplementary measures implemented are effective to prevent that risk.

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 European Union. 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)(c) GDPR, so that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within European Union by the GDPR.

502. Finally under this issue, it is necessary to address certain submissions made by TikTok Ireland concerning the possibility of adopting a risk based approach to the assessment of transfers under Article 46 GDPR.[220] While TikTok Ireland's position is that its Data Transfer Assessments were not contingent on such an approach, it argued that it is permissible to adopt a risk based approach and that this approach reinforces its position that the Data Transfers were lawful. The DPC will address these submissions here.

503. The effect of TikTok Ireland's submissions in this regard is that, when assessing whether the impact of a law or practice in effect in a third country on the rights and freedoms of data subjects in the European Union, it is necessary to take into account the likelihood in practice of an interference in the specific circumstances of the transfer. Its essential argument is that:

(i) The specific circumstances of the transfer includes a consideration of the likelihood and severity of risks to data subjects. When considering the impact of laws and practices in effect in a third country, it is necessary to analyse the likelihood of interferences such as disclosure requests being made by a public authority in practice, rather than the legal interpretation of an applicable law or practice by itself.

(ii) The likelihood or severity of the risk of a disclosure request being made in practice should be determined based on objective factors, such as the documented practical experience of the data importer, together with other relevant, objective elements, which need to be considered carefully to determine whether they carry sufficient weight to enable the data exporter to conclude that the data importer will not be prevented from complying with the SCCs. Other objective elements can include publicly available, or otherwise accessible, reliable information on the existence or absence of disclosure requests within the same sector and / or the application of the law in practice, such as case law and reports by independent oversight bodies. TikTok submits that such objective elements can also include whether the data itself is likely relevant to the public authority, government policy regarding the interpretation of the law and the law itself.

(iii) TikTok Ireland considers that this approach is consistent with the GDPR, the general principle of proportionality in EU law, the case law of the CJEU, including the *Schrems II* judgment, and 2021 SCCs, and is not excluded by the Supplementary Measures Recommendations.

(iv) TikTok Ireland considers that a risk based approach is supported by the DPC's approach to this issue in the Statement of Issues, which asked whether, and the extent to which the 2010 SCCs and the 2021 SCCs "*are not being complied with, or cannot be complied with*", by the China Group Entities.

(v) TikTok Ireland submits that there are a range of objective factors that mean it is extremely unlikely in practice that a Chinese authority would have any interest in or request to get access to EEA user data in the context of the transfers the subject matter of the Inquiry. These factors relate, in large part, to the specific circumstances of the transfer, and the technical, contractual and organisational measures implemented by TikTok Ireland as supplementary measures.

504. TikTok Ireland's submissions in response to the Preliminary Draft Decision elaborated on the factors that it considers make it unlikely in practice that Chinese authorities would access EEA User Data:

> The decision of the CJEU in Schrems II does not require that appropriate safeguards provide an iron-clad guarantee that foreign state agencies have no legal power to access EEA User Data, such that any

[220] TikTok Ireland's Submission dated 19 December 2022, at pages 8–18 relating to the updated position under the 2021 SCCs.

such access could never occur or be absolutely prevented. Rather, the risks arising from data transfers are to be evaluated under a standard of proportionality, rather than perfection, and regard may be had, not only to the likelihood of a potential risk arising at all, but also to the severity of the risk posed were it to arise.

Thus, applying the risk-based approach means that a suspension of the Data Transfers is not required in the event that any risk, no matter how theoretical or remote, is identified; risks which are hypothetical or very unlikely to materialise in practice can be disregarded. It also means that, where a potential risk is identified, it is also permissible to have regard to the severity of the risk posed to the rights and freedoms of data subjects.

The test articulated in Schrems II is whether, in the specific circumstances of the Data Transfers, TikTok's appropriate safeguards incorporate "effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law". Accordingly, it is necessary to have regard both to the applicable laws and practices in China.

It is submitted that a risk-based approach, properly applied, leads inexorably to the conclusion that the transfers can proceed without infringing Article 46(1) GDPR, given that:

1) There is no reason to believe a China Group Entity would, in practice, be compelled to disclose EEA User Data as:

a) Professor Xu and Clifford Chance have confirmed, in the Second Xu Opinion and Clifford Chance Report respectively, that they are not aware of Chinese authorities seeking in practice to compel entities or individuals in China to disclose data stored outside China.

b) Were a Chinese authority to do so, this would contravene Chinese law and government policy.

c) It is very unlikely that EEA User Data would be of interest to a Chinese authority in circumstances where the TikTok Platform does not operate in China and the data by definition relates to users in the EEA, especially once the In-Progress Measures have been implemented to pseudonymise any Accessible Data to which employees of China Group Entities may have access.

d) TikTok has already implemented New Measures which mean that China Group Entities and their employees no longer have access to [redacted] stored in the European Enclave. Further, once the In-Progress Measures are operational, China Group Entities and their employees will not have access to any Protected Data (whether New Protected Data or Legacy Protected Data), and their access to [redacted]

e) As confirmed by the Monthly Reports, monthly transparency reports and in testimony by TikTok's CEO to the US Congress, the China Group Entities have never received a request from a Chinese authority for EEA User Data (and neither has TikTok).

2) The alleged risk that a Chinese authority will compel disclosure of EEA User Data is therefore hypothetical and not based on any actual evidence.

3) Even if this hypothetical risk were to ever materialise, a China Group Entity would, in accordance with Chinese law, push back on any such request and not provide EEA User Data in response to it (as they have legally committed to do in the Intra-Group Agreement and the [redacted].

4) The EEA User Data that is the subject of the Data Transfers may only be remotely accessed from China, [redacted]

5) Therefore, the likelihood of this risk materialising is extremely low, and the severity of the risk posed is also low.[221]

505. TikTok Ireland also submitted that it would be an *"isolated, exceptional and rare case for a Chinese authority to actually have legal jurisdiction under Chinese law to request disclosure of EEA User Data to which a China Group Entity has remote access. As a result, it is extremely unlikely that a Chinese authority would make a request in the first place."*[222]

506. TikTok Ireland submits, further, that this is demonstrated in practice by the fact that TikTok Ireland has never received a disclosure request from law enforcement or governmental authorities in China for EEA User Data, either directly or through a request directed to its China Group Entities.

507. To evidence this for the purposes of the Inquiry, TikTok Ireland has provided:

(i) its Monthly LERT Report from 20 April 2021 to 20 May 2022, and[223]

(ii) its Monthly LERT Report from 20 April 2021 to 20 August 2022,[224]

508. TikTok Ireland has also referred the DPC to the Transparency Reports published at least bi-annually on its website.[225] Prior to the Preliminary Draft Decision, the DPC reviewed the Transparency Reports for H1 2019, H2 2019, H1 2020, H2 2020, H1 2021, H2 2021, and H1 2022, and confirmed that these Reports do not refer to law enforcement requests received from China.

509. TikTok Ireland also referred by way of comparator to the transparency reports published by LinkedIn, which, it submits, record only a very limited number of requests from China. TikTok Ireland submits that LinkedIn's transparency reports[226] indicate that LinkedIn received just 15 requests from Chinese authorities since 2018 and rejected 7 of them. TikTok links this to the fact that up until recently the LinkedIn platform was available in China, whereas the TikTok platform is not made available in China.[227]

510. TikTok Ireland further states that under Chinese law, a Chinese authority is required to follow a mutual judicial assistance process in order to obtain access to data held outside China. It also submits that, even in the limited and exceptional scenarios where one of the China Group Entities were to receive a law enforcement request,

---

[221] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraphs 293 - 296
[222] TikTok Ireland's Response dated 20 June 2022, at page 26.
[223] TikTok Ireland's Response dated 17 June 2022, Schedule A, Document 4.
[224] TikTok Ireland's Submission dated 15 September 2022, Schedule A.
[225] <https://www.tiktok.com/transparency/en/>
[226] https://about.linkedin.com/transparency/government-requests-report.
[227] TikTok Ireland's Submission dated 15 September 2022, at page 14.

it would be legally entitled to redirect the request to TikTok Ireland, in the first instance, or, if the public authority refused to redirect the request, to refuse it.

511. The DPC has carefully considered TikTok Ireland's submissions arguing, in the alternative, for the permissibility of the risk based approach it has outlined. As set out above, the standard that must be complied with requires the data controller to verify, guarantee and demonstrate that the transferred personal data will be subject to an essentially equivalent level of protection to that provided in the EU. Where, as determined by TikTok Ireland, the law and practices of the third country concerned do not ensure an essentially equivalent level of protection to that guaranteed in the EU, even when SCCs are used, it becomes relevant to determine whether any supplementary measures are capable of compensating for the lack of data protection in that third country. As appearing from the Supplementary Measures Recommendations, the supplementary measures implemented should *"prevent the risk of potential application"* of problematic legislation in effect in the third country to the transfers.[228] The nature and extent of the risk to data subjects arising from the deficiencies identified in the legal framework of the third country concerned may then be relevant to determining the supplementary measures that are needed, and therefore it is important, at the outset, that such risks are identified and clearly defined. In this regard, a data controller's assessment of risk as *"theoretical or remote"* or *"hypothetical or very unlikely to materialise"*, may be relevant in the particular circumstances to that data controller's selection of supplementary measures to verify, guarantee and demonstrate an essentially equivalent level of protection.

512. However, in the particular circumstances of this Inquiry, contrary to TikTok Ireland's submissions, TikTok Ireland has not established that the risk of Chinese authority access to EEA User Data the subject of the Data Transfers is *"theoretical or remote"*, or *"hypothetical or very unlikely to materialise in practice"* and the DPC does not accept TikTok Ireland's submission that the risks can be disregarded. The DPC considers that the risks of potential access is a significant concern. As outlined above, TikTok Ireland's assessments and conclusions regarding the territoriality principle failed to clarify whether, and the extent to which, problematic laws may apply in the context of the transfers, and consequently failed to set out in a clear way the deficiencies it acknowledges to exist in the Chinese legal framework. TikTok Ireland's assessment of the territoriality principle failed to consider the issue of Chinese authorities obtaining access to EEA User Data that was routinely transferred to China and that was temporarily processed in China to facilitate the remote access. TikTok Ireland also failed to provide sufficient consideration to how the divergences that it acknowledges to exist in the Chinese legal framework could apply to EEA User Data subject to the Data Transfers. As set out above, this includes a failure on TikTok Ireland's part to define the scope of the divergence from EU Law caused by the confidentiality obligations that can be imposed pursuant to Chinese law and how the divergence could impact EEA User Data that is processed in China. Therefore, TikTok Ireland has not established that the risk of Chinese authority access to EEA User Data the subject of the Data Transfers is *"theoretical or remote"*, or *"hypothetical or very unlikely to materialise in practice"*. TikTok Ireland is not in a position to demonstrate that, notwithstanding the deficiencies in Chinese law established in its Data Transfer Assessments, in fact, no interference with EU rights occurs. For the reasons set out in this Decision, TikTok Ireland has failed to verify, guarantee and demonstrate that the supplementary measures and the SCCs were effective to ensure that the personal data of EEA Users was afforded a level of protection essentially equivalent to that guaranteed within the EU.

[228] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021), at pages 17-18.

H. Issue 4 – Article 49 Derogations

513. Issue 4 in this Inquiry concerns whether TikTok Ireland relied on the derogations set out in Article 49 GDPR for the Data Transfers, and if so, the lawfulness of same.

514. TikTok Ireland's response to the Preliminary Draft Decision confirmed that it did not rely on the Article 49 Derogations in respect of the Data Transfers up to and including the date upon which those submissions were made, 9 September 2023. TikTok Ireland relied exclusively on Article 46 GDPR for the Data Transfers during the temporal scope of this inquiry. Accordingly, the DPC finds that the Data Transfers subject to this Decision were not made in reliance on any of the derogations under Article 49 GDPR. Therefore, Article 49 GDPR did not legitimise the Data Transfers.

515. Notwithstanding that TikTok Ireland has not relied on Article 49 GDPR for the Data Transfers, it submitted to the inquiry that it reserves its entitlement to rely on the derogations if the DPC finds that TikTok Ireland cannot lawfully transfer the personal data subject to the Data Transfers in reliance on Article 46 GDPR. TikTok Ireland contended to the Inquiry that it is entitled to rely on the derogations in respect of contractual necessity pursuant to Article 49(1)(b) GDPR and of compelling legitimate interests pursuant to the second subparagraph of Article 49(1) GDPR for certain of the transfers of EEA User Data. TikTok Ireland also stated that it reserved its entitlement to rely on consent in accordance with Article 49(1)(a).

516. TikTok Ireland also submitted that:

> Since the Article 49 Facts are that TikTok does not rely on Article 49 GDPR derogations for its Data Transfers, it follows that the DPC has no basis for making any Article 49 Lawfulness finding in respect of TikTok's Data Transfers based on the Article 49 Facts.[229]

517. The DPC accepts TikTok Ireland's position that it did not rely on the derogations during the temporal scope of the Inquiry. However, having regard to TikTok Ireland's submissions regarding its entitlement to rely on the derogations if the DPC finds that it cannot lawfully transfer the personal data subject to the Data Transfers in reliance on Article 46 GDPR, the DPC considers it appropriate to address TikTok Ireland's contended entitlement to rely on those derogations for the Data Transfers going forward. Below, the DPC will assess TikTok Ireland's potential reliance on Article 49(1)(a), Article 49(1)(b) and the second subparagraph of Article 49(1) GDPR for the Data Transfers.

Article 49 GDPR

518. Article 49(1) GDPR, first subparagraph, provides:

> 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

[229] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 318.

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

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

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

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

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

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

519. Article 49(1) GDPR, second subparagraph, provides:

> Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

520. Article 49(6) GDPR provides:

> The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Requirement to interpret Article 49 GDPR in light of the Charter

521. Article 52 of the Charter recognises that the rights and freedoms recognised by the Charter may be limited, but any such limitation must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, the limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

522. Article 52(1) therefore identifies three cumulative requirements with which any limitation on or derogation from a Charter right must comply. Derogations are permissible only where they, first, are provided for by law, second, respect the 'essence' of that freedom and, third, respect the principle of proportionality.

Requirement to interpret derogations restrictively

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

524. First, the CJEU has confirmed that the protection of fundamental rights guaranteed under the Charter requires that derogations from and limitations on those rights must apply only in so far as is strictly necessary, and must be narrowly construed.[230]

525. Second, and relatedly, it is well established that derogations cannot be interpreted so as to allow the exception provided by the derogation to replace the rule established by the EU measure. It is necessary that the exception remain an exception.

526. In that respect, where a provision *"provides for an exception to the general rule [it must] be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle […] to become the rule, if [the rule] is not to be rendered largely meaningless."*[231]

527. Third, the CJEU has confirmed that:

> […] the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances […] and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter.[232]

Derogation under Article 49(1)(a) GDPR

528. TikTok Ireland's submissions on the Preliminary Draft Decision stated:

---

[230] See, e.g., the judgment of the CJEU Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů*Ryneš,* judgment of 11 December 2014 (ECLI:EU:C:2014:2428), paragraphs 28 –30.
[231] See judgments of the CJEU: Case C-140/20, *G.D. v. An Garda Siochána,* judgment of 5 April 2022 (EU:C:2022:258),at paragraph 40; Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, judgment of 21 December 2016 (ECLI:EU:C:2016:970) at paragraph 89; Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others*, judgment of 6 October 2020, (ECLI:EU:C:2020:791), at paragraph 111.
[232] Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministres, j*udgment of 21 June 2022 (ECLI:EU:C:2022:491), at paragraph 114.

Finally, as noted above, TikTok reserves the entitlement to also rely as appropriate on consent in accordance with Article 49(1)(a) GDPR should it prove necessary and appropriate to do so. As matters currently stand, however, TikTok does not do so.[233]

529. Article 49(1)(a) GDPR provides for transfers to take place where the data subject has explicitly consented to the proposed transfer.

530. TikTok Ireland did not obtain the explicit consent of EU/EEA users to any of the Data Transfers prior to or during the temporal scope of this inquiry. It follows, therefore, that TikTok Ireland cannot rely on the derogation under Article 49(1)(a) GDPR to justify the Data Transfers during the temporal scope.

531. Whether TikTok Ireland could rely on Article 49(1)(a) GDPR to justify any of the Data Transfers in the future, if it were to obtain the explicit consent of EU/EEA users, cannot be determined in the abstract.

532. However, it is important to note that in order to obtain explicit consent under Article 49(1)(a) GDPR to the proposed transfer, it is necessary that the data subject is informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

533. As set out above, the Data Transfers considered in this Inquiry concerned remote access to personal data of EEA Users of the TikTok platform to China by personnel of the China Group Entities. The Data Transfers occurred regularly within this stable relationship between TikTok Ireland and the China Group Entities. The Remote Access Solution enabled staff of the China Group Entities to access EEA User Data to provide functions such as research and development, security, analytics, online payments, and customer and technical support. The nature of this processing concerned diverse matters relating to monitoring content trends, testing, and protecting the platform from fraudulent payments. As set out in the 2021 and 2022 Data Transfer Assessments, this resulted in a broad range of categories of personal data being transferred to China by means of remote access. Therefore, it is clear the Data Transfers concerned systematic, repetitive, and continuous transfers of personal data to China. The Data Transfers cannot be considered occasional or not-repetitive.

534. The DPC further notes that following the implementation of Project Clover, the Data Transfers remain systematic, repetitive and continuous. These transfers concern remote access to *"Allowable Data"* by personnel of the China Group Entities. The purposes of these ongoing transfers include content delivery, customer and technical support, security, research and development, analytics, online payments, and content moderation. On a continuing basis, this results in a broad range of categories of personal data being transferred to China by means of the remote access. These categories are set out in the section of this Decision detailing the order suspending data flows pursuant to Article 58(2)(j) GDPR. The nature of the processing is also broad and includes troubleshooting, fixing issues in the production system, viewing testing results, analysing data; developing, testing, maintaining and optimising machine learning models and algorithms; reviewing customer feedback tickets to understand the nature of specific technical issues, triaging these issues, routing to the appropriate engineering (or payment) team if necessary; and reviewing of moderation outputs to determine how overall efficiency and effectiveness can be improved, and for capacity planning and training purposes. Therefore, it is clear the Data Transfers on an ongoing basis concern systematic, repetitive, and continuous transfers of personal data to China. Therefore, the Data Transfers cannot be considered occasional or not-repetitive.

[233] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 359.

535. It is unclear how, on a practical level, TikTok Ireland could justify the systematic, repetitive, and continuous transfers on the basis of a scheme by which the explicit consent of EEA Users to any proposed transfer of their personal data to China was obtained. In particular, the DPC finds that a single consent by a data subject could not be sufficient to justify any and all future transfers of that user's personal data to China.

536. In that regard, there is a high threshold for obtaining any consent under the GDPR. The threshold for obtaining consent under Article 49(1)(a) GDPR is even higher. In particular:

a. The data subject must have *"explicitly consented"* to *"the proposed transfer"*, and

b. The data subject must have been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

537. The DPC notes in this regard – and agrees with – the statement in the EDPB Guidelines that:

> Consent must be specific for the particular data transfer/set of transfers
>
> One of the requirements of valid consent is that it must be specific. In order to constitute a valid ground for a data transfer pursuant to Article 49(1)(a), hence, consent needs to be specifically given for the particular data transfer or set of transfers.
>
> …
>
> Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer at the time of the collection of the data, e.g. if the occurrence and specific circumstances of a transfer are not known at the time consent is requested, the impact on the data subject cannot be assessed.[234]

538. The DPC finds that the requirement that consent be *"explicit"* and that it relate to *"the proposed transfer"* precludes a single consent being obtained for continuous and ongoing data transfers and/or different sets of transfers. The DPC is also of the view that seeking a single open-ended consent for continuous and ongoing data transfers and/or different sets of transfers is not compatible with the obligation to inform the data subject of the possible risks of the transfers being made.

Derogation under Article 49(1)(b) GDPR

539. The derogation in Article 49(1)(b) GDPR refers to transfers which are *"necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request"*.

540. TikTok Ireland has suggested that, in some circumstances, the derogation under Article 49(1)(b) GDPR may be one derogation that could potentially apply to the transfers. It has outlined that:

[234] European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018), at page 4.

While the derogations in Article 49 GDPR are distinct from the safeguard mechanisms provided under the GDPR, we note for completeness that, in certain cases, Article 49 GDPR derogations may be applicable and relevant depending on the facts of the particular case.

For example, in order for TikTok to perform its contract with its users and provide the Platform (i.e. the service to EEA Users), it is necessary to permit limited remote access to EEA User Data to authorised personnel of ByteDance group entities to perform the services described in response to Query 3, such access being necessary to provide the Platform to EEA Users. For example, engineering teams in China investigate and remediate functionality issues, including those reported by EEA Users, across all of the core TikTok features. Without this access and these personnel performing these functions, TikTok would not be able to provide its Platform to EEA Users. Further, from a practical service perspective, access from engineering personnel in China is necessary in order for them to address any product issues which may arise during hours when EU-based (and US-based) engineering staff are not working. Therefore, while TikTok relies on SCCs (bolstered by supplementary measures) for transfers to certain ByteDance group entities based in China ("China Group Entities"), the derogation under Article 49(1)(b) may be applicable in some cases.[235]

541. TikTok has further clarified that:

To date, Tiktok has not needed to rely on the derogations in Article 49 GDPR in relation to the Transfers. This is because TikTok relies on appropriate safeguards under Article 46 GDPR and Article 49 GDPR only applies in the absence of an adequacy decision or appropriate safeguards pursuant to Article 46 GDPR. In section 4.4 of the October 2021 Response, TikTok reserved the right to make further submissions in relation to the Article 49 GDPR derogations generally, as necessary and appropriate. TikTok continues to reserve its right in this regard but would like to clarify that it currently only relies on the 2010 SCCs, augmented by supplementary measures, as an appropriate safeguard in accordance with Article 46 GDPR to provide authorised remote access to personnel in China to EEA User Data pursuant to the Intra-Group Agreement. This is on the basis of TikTok's understanding that, in the specific circumstances of the Transfers, the 2010 SCCs provide a valid means for the Transfers in compliance with Chapter V GDPR. It is only in the event that the 2010 SCCs were found not to provide a valid legal basis to make the Transfers that it would be necessary to address the availability of the Article 49 derogations and TikTok reserves its right to do so.[236]

542. TikTok Ireland confirmed the above position in its submission dated 15 September 2022, indicating that *"[it] is only in the event that the DPC finds that TikTok cannot rely on the 2010 SCCs (or, as applicable, 2021 SCCs), complemented and augmented by supplementary measures, as an appropriate safeguard in accordance with Article 46 GDPR for Remote Access, that TikTok reserves the right to rely on one or more of the Article 49 GDPR derogations."*[237]

[235] TikTok Ireland's Response dated 12 October 2021, at pages 2–3.
[236] TikTok Ireland's Response dated 20 June 2022, at page 19.
[237] TikTok Ireland's Response dated 15 September 2022, at page 5.

543. TikTok Ireland's 2023 submissions in response to the Preliminary Draft Decision set out more limited specific circumstances in which it contends the derogations would apply *"on an emergency or exceptional basis"*. Those situations include:

1. an anomalous and unexplained dip in content moderation levels that, if not resolved urgently, could result in EEA Users being exposed to inappropriate or harmful content through the Platform;
2. an unexpected and material degradation of TikTok's security on the Platform, or a degradation of TikTok security that has endured over a protracted period; and
3. a significant number of users experiencing Platform outages, Platform crashes, an inability to publish or consume videos, or transaction or payment settlement issues in TikTok LIVE.[238]

544. TikTok Ireland outlined that such situations could require that highly skilled TikTok engineers in the China Group Entities need remote access to EEA User Data on an emergency or exceptional basis to ensure the TikTok service continues to be available to EEA Users and provides a safe experience for them (e.g. where TikTok becomes aware of a serious Platform issue that significantly affects EEA Users and/or gives rise to risk of harm to EEA Users).

545. TikTok Ireland submitted that the particular Article 49(1) GDPR derogation that TikTok would rely on in the above circumstances would depend upon the nature, context, purpose and scope of the issue arising and remote access required. However, TikTok considers that, in such circumstances, it might rely upon the derogations in respect of either contractual necessity pursuant to Article 49(1)(b) GDPR or compelling legitimate interests pursuant to the second subparagraph of Article 49(1) GDPR.

546. Regarding its reliance on contractual necessity under Article 49(1)(b), TikTok Ireland referred to its contractual commitment to EEA Users in its Terms of Service whereby it *"[promises] to provide the Platform to you with reasonable skill and care and to act with professional diligence for so long as we choose to offer the Platform. We will also take all reasonable steps to keep the Platform a safe and secure environment for our users"*.

547. TikTok Ireland submitted that:

> Failure to provide remote access in the circumstances described above would fall short of TikTok's contractual commitment "to provide the Platform with reasonable skill and care and to act with professional diligence", and "to take all reasonable steps to keep the Platform a safe and secure environment" for EEA Users. Put another way, the granting of remote access to its specialist engineers in the China Group Entities on an emergency or exceptional basis in the circumstances described above would be "objectively indispensable" to enable TikTok to perform its contract with EEA Users.
>
> Consequently, TikTok submits that remote access by specialist engineers in China Group Entities on an emergency or exceptional basis in the circumstances described above would satisfy the contractual necessity criteria set out in GDPR Article 49(1)(b).[239]

548. [redacted]

[238] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 342.
[239] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraphs 351 and 352.

[redacted]

549. It is clear that derogations such as that provided for by Article 49(1)(b) must be interpreted narrowly, and any restrictions or derogations from the rights guaranteed in Articles 7 and 8 of the Charter will be permissible only insofar as strictly necessary. Such an interpretation is necessary to avoid a situation in which the exception may become the rule. The DPC finds that TikTok Ireland has not demonstrated that such transfers would be strictly necessary for the performance of the contract between TikTok Ireland and its users.

550. Furthermore, Recital 111 GDPR states that transfers made on the basis of the *"contractual necessity"* and *"legal claims"* derogations in Article 49(1)(b), (c) and (e) should be occasional. The EDPB states in this regard that:

> The EDPB notes that the term "occasional" is used in recital 111 and the term "not repetitive" is used in the "compelling legitimate interests" derogation under Article 49 par. 1 §2. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive. Besides, a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.[240]

551. The EDPB goes on to state that:

> [i]n general, although the derogations relating to the performance of a contract may appear to be potentially rather broad, they are being limited by the criterions of "necessity" and of "occasional transfers".[241]

552. TikTok Ireland submitted that the requirement that transfers can only be made in reliance on the derogation in Article 49(1)(b) GDPR in respect of contractual necessity if those transfers are occasional is not supported by the text of Article 49. TikTok Ireland submitted that conditions on the availability of each of the derogations are expressly identified in Article 49(1) GDPR, and, in those circumstances, no other conditions can be implied whereby the availability of specific derogations is limited to conditions that are not specifically identified. TikTok Ireland also submitted that Recital 111, as a mere Recital, cannot be relied upon to constitute a rule not provided for in the text of the GDPR and that a recital to a regulation cannot be relied on to interpret an operative provision of the regulation in a manner inconsistent with the language of the provision itself.

553. For the reasons that follow, the DPC does not accept TikTok Ireland's submissions in this regard. The DPC acknowledges that recitals to the GPDR do not have the same status as the regulation's operative provisions.

---

[240] European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018), at page 4.
[241] European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018), at page 8.

The recitals do not have binding legal force and cannot be relied on as a ground for either derogating from the actual provisions of the act, or for interpreting those provisions in a matter that is clearly contrary to their wording. This is well established in the CJEU jurisprudence.

554. However, the CJEU has held that recitals of an EU act '*may explain the content of the provisions of that act',* and that recitals *'constitute important elements for the purposes of interpretation, which may clarify the intentions of the author of that act.'*[242]

555. In that respect, in Confédération paysanne and Others,[243] the CJEU relied on Recital 17 of the GMO Release Directive[244] to inform the limitations of a derogation under that Directive. Article 3(1) of the GMO Release Directive provides that the Directive shall not apply to organisms obtained through the techniques of genetic modification listed in Annex 1 B. One of the techniques listed in Annex 1 B is '*mutagenesis*'.

556. No limitation on the type of mutagenesis excluded from the scope of the Directive is contained in Article 3 or Annex 1 B. The CJEU nevertheless interpreted the limitations on the scope of that derogation in light of Recital 17, which provides:

> This Directive should not apply to organisms obtained through certain techniques of genetic modification which have conventionally been used in a number of applications and have a long safety record.

557. In light of that Recital the CJEU held:

> Article 3(1) of Directive 2001/18, read in conjunction with point 1 of Annex I B to that directive and in the light of recital 17 thereof, must be interpreted as meaning that only organisms obtained by means of techniques/methods of mutagenesis which have conventionally been used in a number of applications and have a long safety record are excluded from the scope of that directive.

558. In reaching that conclusion the CJEU relied on, inter alia, the following:

> a. That as "a provision derogating from the requirement to subject GMOs to the obligation laid down in the Directive", Article 3(1), read in conjunction with Annex 1 B, "must be interpreted strictly";
>
> b. That for the purpose of interpreting a provision of EU law, it is necessary to consider not only its wording but also "the context in which it occurs and the objectives pursued by the rules of which it is part";
>
> c. That by "referring generally to mutagenesis", that provision does not, on its own, "provide any conclusive guidance as to the types of techniques/methods that the EU legislature intended specifically to exclude from the scope of the directive";

---

[242] Case C-418/18, Patrick Grégor Puppinck and Others v European Commission, judgment of 19 December 2019 (ECLI:EU:C:2019:1113), at paragraph 75.
[243] Case C-528/16, Confédération paysanne and Others v Premier ministre and Ministre de l'agriculture, de l'agroalimentaire et de la forêt, judgment of 25 July 2018 (ECLI:EU:C:2018:583).
[244] Directive 2001/18/EC of the European Parliament and of the Council of 12 March 2001 on the deliberate release into the environment of genetically modified organisms and repealing Council Directive 90/220/EEC.

d. That the EU legislature set out in recital 17 "the conditions under which certain GMOs should be excluded from the scope of the Directive" and that, "accordingly, the scope of the derogation … must be determined in the light of the clarifications thus given by the EU legislature"; and

e. That an interpretation of the derogation that did not exclude techniques that had not conventionally been used in a number of applications and have a long safety record would fail to have regard to the intention of the EU legislature, reflected in recital 17, and would compromise the objective of the Directive.

559. While the DPC accepts that a recital cannot be relied on to derogate from the actual provisions of the act in question, or to interpret those provisions in a manner that is clearly contrary to their wording, the DPC does not accept that Recital 111 of the GDPR either derogates from Article 49(1)(b) GDPR nor results in an interpretation of Article 49(1)(b) GDPR that is clearly contrary to its wording. Rather, recital 111 of the GDPR serves to clarify the scope of the derogation permitted under Article 49(1)(b) GDPR.

560. The EU legislature set out in Recital 111 of the GDPR the conditions under which certain transfers should be excluded from the requirements in GDPR Chapter IV and accordingly, the scope of the derogation must be determined in the light of the clarifications thus given by the EU legislature. The DPC is satisfied that interpreting the limitations of the scope of Article 49(1)(b) GDPR in light of Recital 111 of the GDPR is entirely consistent with the approach taken by the CJEU in Confédération paysanne.

561. The DPC finds that Article 49(1)(b) GDPR can relied on to justify occasional transfers only. The DPC finds that the contractual necessity derogation cannot be relied on to justify the systematic, repetitive and continuous transfers to China within the Data Transfers.

562. Furthermore, regarding the hypothetical scenarios outlined by TikTok Ireland in which it contends that it would rely on the derogations for more limited circumstances under Article 49, including those which TikTok Ireland described as *"emergency or exceptional"*, the DPC does not consider that TikTok Ireland has demonstrated that transfers would meet the requirement of being occasional in nature. [redacted] Furthermore, the issues outlined appear repetitive and continuous in nature in circumstances where they relate to matters that typically arise repeatedly for large technology platforms such as TikTok Ireland. [redacted]

Derogation under the second subparagraph of Article 49(1)

563. The second subparagraph of Article 49(1) states that a transfer based on that subparagraph may take place only if the transfer is not repetitive. That subparagraph also requires that the controller shall inform the supervisory authority and the data subject of the transfer; that none of the derogations referred to in the first subparagraph of Article 49(1) is applicable; that the transfer concerns only a limited number of data subjects; and that the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject.

564. The second subparagraph of Article 49(1) also requires the controller to first assess all the circumstances surrounding the data transfer and on the basis of that assessment to provide suitable safeguards with regard to the protection of personal data.

565. The EDPB's Guidelines on derogations provides:

> This layered approach to considering the use of derogations as a basis for transfers requires consideration of whether it is possible to use a transfer tool provided in Article 45 or 46 or one of the specific derogations set out in Article 49 (1) § 1, before resorting to the derogation of Article 49 (1) §2. This can only be used in residual cases according to recital 113 and is dependent on a significant number of conditions expressly laid down by law. In line with the principle of accountability enshrined in the GDPR the data exporter must be therefore able to demonstrate that it was neither possible to frame the data transfer by appropriate safeguards pursuant to Article 46 nor to apply one of the derogations as contained in Article 49 (1) § 1.[245]

566. Whether TikTok Ireland could rely on the second subparagraph of Article 49(1) to justify any data transfers in the future cannot be determined in the abstract. In this regard, the DPC notes that TikTok Ireland has not produced a balancing test between the data exporter's compelling legitimate interest pursued and the interests or rights and freedoms of the data subject. However, the DPC finds that Article 49(1)(b) GDPR can be relied on to justify occasional transfers only. The DPC finds that the second subparagraph of Article 49(1) can be relied on to justify non-repetitive transfers only and cannot be relied on to justify the systematic, repetitive and continuous transfers to China within the ongoing Data Transfers.

567. As set out above, the DPC has concerns regarding the hypothetical scenarios outlined by TikTok Ireland in which it contends that it would rely on the derogations for more limited circumstances under Article 49, including those which TikTok Ireland described as *"emergency or exceptional"*. The DPC does not consider that TikTok Ireland has demonstrated that such transfers would meet the requirement of being occasional in nature, nor that it has demonstrated the necessity of such transfers.

a) Findings in respect of Issue 4

568. The DPC finds that TikTok Ireland cannot rely on the derogations under Article 49 GDPR in respect of the Data Transfers made during the temporal scope, which, as set out above, were systematic, repetitive, and continuous.

I. Finding of Infringement 1

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 by means of the Remote Access Solution 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 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.

---

[245] European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018), at page 14.

J. Issue 5 – Transparency

571. The scope of the Inquiry includes an examination of whether TikTok Ireland can demonstrate in accordance with Article 13(1)(f) GDPR that it has fulfilled its obligations with regard to provision of information to its users in relation to transfers of personal data to China by means of the Remote Access Solution.

572. Recital 39 to the GDPR is particularly relevant to understanding the content of the principle of transparency and provides as follows:

> Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should 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.

573. Article 12(1) GDPR states as follows:

> The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

574. With reference to information to be given in respect of personal data collected from the data subject, Article 13(1)(f) provides:

> 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
>
> […]
>
> (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

575. Recitals 60–62 GDPR are also relevant to interpreting the transparency and information obligations under Article 13 GDPR. In particular, recital 60 provides that:

> The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. 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.

576. The Article 29 Working Party[246] in its guidance (endorsed by the EDPB)[247] highlighted that:

> [t]ransparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights.

577. The transparency principle is important for enabling data subjects to effectively exercise the rights guaranteed by the GDPR. This point was emphasised by the CJEU in its judgment in Bara,[248] where it held, interpreting Articles 6(1)(a) and 10, 11 and 13 of Directive 95/46/EC, that:

> […] the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive.

578. The CJEU adopted an essentially parallel analysis in its judgment in RW v Österreichische Post AG[249] concerning the interpretation of Article 15(1)(c) GDPR, which provides:

> 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
>
> […]
>
> (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations

579. The CJEU held with regard to the obligation in Article 15(1)(c) GDPR that:

> It follows […] that Article 15(1)(c) of the GDPR is one of the provisions intended to ensure transparency vis-à-vis the data subject of the manner in which personal data are processed and enables that person,

---

[246] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP 260 (11 April 2018), at page 5.
[247] European Data Protection Board Endorsement 1/2018 dated 25 May 2018.
[248] Case C-201/14, Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others, judgment of 1 October 2015 (ECLI:*Bara*, EU:C:2015:638), at paragraph 33.
[249] Case C-154/21, RW v Österreichische Post AG, judgment of 12 January 2023, *Österreichische Post,* (ECLI:EU:C:2023:3).

> as the Advocate General observed in point 33 of his Opinion, to exercise the rights laid down, inter alia, in Articles 16 to 19, 21, 79 and 82 of the GDPR.
>
> Accordingly, the information provided to the data subject pursuant to the right of access provided for in Article 15(1)(c) of the GDPR must be as precise as possible. In particular, that right of access entails the ability of the data subject to obtain from the controller information about the specific recipients to whom the data have been or will be disclosed or, alternatively, to elect merely to request information concerning the categories of recipient.[250]

580. This judgment concerns access requests made under Article 15 of the GDPR, which operate in a different context to the proactive obligations under Article 13 GDPR to provide information to data subjects. However, the judgment nonetheless underscores the importance of the provision of meaningful information to data subjects, by means of Articles 13, 15 or otherwise, in the context of enabling data subjects to exercise their rights and to make informed decisions regarding the processing of their personal data. The CJEU held that the interpretation of Article 15(1) GDPR was supported by the overall objective of the GDPR, namely the purpose reflected in recital 10 GDPR of ensuring *"a high level or protection of natural persons within the European Union"*, and of implementing *"the requirements arising from the fundamental right, protected by Article 8 of the Charter of Fundamental Rights of the European Union, to the protection of personal data, in particular the requirements expressly laid down in Article 8(2) thereof".*[251]

581. Returning to the interpretation of Article 13(1)(f) GDPR, the Article 29 Working Party outlined the content of that obligation as follows:

> The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45 / binding corporate rules under Article 47 / standard data protection clauses under Article 46.2 / derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.[252]

582. Fair and transparent processing requires that information provided to data subjects on transfers to third countries under Article 13(1)(f) should be as meaningful as possible – and, indeed, as specific and precise as possible. This is supported, by analogy with the reasoning in Bara and Österreichische Post[253], by the importance of transparency to enabling the effective exercise of data subjects' rights, and by the general objective of the GDPR of fully implementing the right to protection of personal data under Article 8 of the Charter.

---

[250] Case C-154/21, RW v Österreichische Post AG, judgment of 12 January 2023, *Österreichische Post,* (ECLI:EU:C:2023:3), at paragraphs 42–43.
[251] Case C-154/21, RW v Österreichische Post AG, judgment of 12 January 2023, *Österreichische Post,* (ECLI:EU:C:2023:3), at paragraphs 44–45.
[252] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP 260 (11 April 2018), at pages 37-38.
[253] Case C-154/21, RW v Österreichische Post AG, judgment of 12 January 2023, *Österreichische Post,* (ECLI:EU:C:2023:3).

583. While Article 13(1)(f) GDPR does not expressly state that a controller must identify the country of transfer, it is clear that this information must be provided where the circumstances of the transfer are such that the information is necessary to enable data subjects to receive transparent and meaningful information.

584. In this regard, it is important to note that Article 13(1)(f) GDPR governs the information that must be provided to data subjects irrespective of whether the transfers are based on an adequacy decision under Article 45, appropriate safeguards under Article 46, or derogations under Article 49. For example, Article 13(1)(f) GDPR requires that, where a controller transfers personal data on the basis of an adequacy decision, the controller must inform the data subject of the existence of that adequacy decision. In such circumstances, to comply with Article 13(1)(f), the controller must enable the data subject to identify which adequacy decision is being relied upon. Therefore, in such circumstances, in order to provide meaningful information, it may not be necessary to separately articulate the country of transfer as such information may be implicit where the controller has properly enabled the data subjects to identify the adequacy decision being relied upon.[254]

585. However, where a controller transfers personal data to a third country on the basis of appropriate safeguards under Article 46 GDPR, its does so on the basis that there is no relevant adequacy decision available under Article 45(3) GDPR. Furthermore, in transfers such as those made by TikTok Ireland during the temporal scope, where the controller is making transfers to a third country wherein the legal framework in that country has issues that would preclude a finding of essential equivalence to EU law in the absence of supplementary measures, it is essential pursuant to Article 13(1)(f) that the data controller identifies the country of transfer. If such information is not provided, data subjects would be denied transparent and meaningful information regarding the transfers. In such circumstances, it is crucial that the data subjects are enabled to make decisions regarding their engagement with entities where that engagement may result in their data being transferred to a specified third country.

586. In summary, the obligation under Article 13(1)(f) GDPR, read with recitals 39 and 60, and Article 12(1) GDPR, requires a controller to:

(i) Inform data subjects of the fact that the controller intends to transfer personal data to a third country and, in general, to specify the third country to which the personal data will be transferred.

(ii) Specify the transfer mechanism (whether, for example, an adequacy decision under Article 45, binding corporate rules under Article 47, SCCs under Article 46(2)(c), or derogations under Article 49 GDPR).

(iii) Provide a reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(iv) Take appropriate measures to provide that information to data subjects, in an intelligible and easily accessible form, using clear and plain language, in writing, or by other means, including, where appropriate, by electronic means. (In this regard, the Article 29 Working Party has recommended

[254] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision referred to the DPC's Decision of 20 August 2021 in Inquiry IN-18-12-2 as authority for the proposition that Article 13(1)(f) does not require a data controller to identify the country of transfer. TikTok Ireland's submissions in this regard have misconstrued that Decision in circumstances where extracts from the that Decision relied upon by TikTok Ireland concern, inter alia, a finding of infringement of Article 13(1)(f) regarding data subjects' ability to identify which adequacy decision was being relied upon in that case.

that in the case of a controller with an online presence, an online layered privacy notice should be provided, that enables users to navigate to particular aspects of the notice that are of most interest to them).[255]

(v) Provide that information to data subjects in a timely manner, at the time when the personal data is obtained from a data subject.

a) TikTok's October 2021 EEA Privacy Policy

587. The DPC was directed in TikTok Ireland's 2021 submissions[256] to a link to TikTok's EEA Privacy Policy that was updated on 5 October 2021 ("the October 2021 EEA Privacy Policy").

588. In the section entitled 'How We Share Your Information', the EEA Privacy Policy stated (with hyperlinked content underlined):

> As a global company, our Services are supported by a number of affiliated entities within our corporate group ("Corporate Group"). We share Information You Provide, Automatically Collected Information, and Information From Others with our Corporate Group as necessary to enable them to provide important functions such as cloud hosting, content delivery, security, research and development, analytics, online payments, customer and technical support, and content moderation.

589. In the section entitled 'Our Global Operations and Data Transfers', the EEA Privacy Policy stated (with hyperlinked content underlined):

> 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.

590. In response to the DPC's Statement of Issues, TikTok Ireland further submitted, in respect of the 2021 EEA Privacy Policy, that:

---

[255] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP 260 (11 April 2018), at pages 11 and 14.
[256] TikTok Ireland's Response dated 12 October 2021, at pages 1 and 19.

6.5 In short, TikTok explains to EEA Users:

(A) the fact that TikTok intends to (and does) transfer personal data to a third country (i.e. a destination outside of the EEA);

(B) the fact that TikTok intends to (and does) transfer personal data to entities in its Corporate Group;

(C) that TikTok relies on SCCs (i.e. appropriate safeguards) for these transfers where there is no adequacy decision; and

(D) the means by which EEA Users can obtain a copy of these appropriate safeguards (i.e. the SCCs).

6.6 This information enables EEA Users to understand whether and how their data will be transferred outside of the EEA. Therefore, TikTok's approach to its provision of information to EEA Users on personal data transfers aligns with the objective and text of Article 13(1)(f) GDPR.

6.7 Article 13(1)(f) GDPR does not require controllers to name the third country(ies) to which personal data is transferred using SCCs nor does it require controllers to name all or any third countries where EEA personal data is in transit through remote access sessions.

6.8 The relevant information regarding data transfers in the Privacy Policy:

(A) is set out in an easily accessible and concise form through the use of the clear heading "Our Global Operations and Data Transfers" - this allows Users to easily navigate to the issues of data transfers which may be of interest to them - and through the use of bullet points; and

(B) uses clear and plain language.[257]

591. The DPC has reviewed the English language version of the October 2021 EEA Privacy Policy, which is a layered privacy policy that the DPC considers, in this context, is an appropriate measure for providing the information required by Article 13(1)(f) GDPR to users of the TikTok platform. However, the DPC finds that the content of the information provided by the October 2021 EEA Privacy Policy to EEA users was inadequate in two key respects for the purposes of Article 13(1)(f) GDPR.

592. 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

[257] TikTok Ireland's Submission dated 15 September 2022, at page 25.

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 subjects *"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.[258]

593. 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.

594. 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.

595. In this case, during the temporal scope, the processing included 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[259], a basic factual description of these 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."* As set out above, the material scope of this Decision does not include TikTok Ireland's transfers that resulted in EEA User Data being stored on servers in China, and this Decision does not consider or make any findings regarding TikTok Ireland's compliance with its transparency obligations in that regard.

596. TikTok Ireland submitted that the DPC's findings result in a situation whereby *"less information is required to be provided to data subjects for more intrusive processing (i.e. a direct transfer), whereas more information is required to be provided to data subjects in respect of less intrusive processing (i.e. where there is remote access only)."*[260] However, this submission misconstrues the nature of the obligation under Article 13(1)(f). As set out above, in order to comply with the obligation on controllers to inform data subjects of the fact that the controller intends to transfer personal data to a third country or international organisation, the data subjects must be provided with meaningful information as to the nature of the processing operations that constitute the transfer. The obligation rests with each controller to provide such information in a concise,

---

[258] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP 260 (11 April 2018), at page 7.

[259] Article 12(1) GDPR requires controllers to take appropriate measures to provide any information referred to in Article 13 GDPR to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

[260] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 397.

transparent, intelligible and easily accessible form, using clear and plain language. It is not correct to state that there is a link between the intrusiveness of the processing and the amount of information that must be provided under Article 13(1)(f). Rather, the obligation is to provide information that is transparent and meaningful in respect of those processing operations. The complexity of the processing may have a bearing on the amount of information that must be provided in order for the information to be meaningful to the data subjects. However, in such circumstances, the obligation to provide the information in a concise form still applies. In the circumstances of TikTok Ireland's transfers of personal data to China during the temporal scope, it is clear that TikTok Ireland was obliged to provide a basic factual description of how the transfers consisted of remote access to personal data stored in Singapore and the United States by personnel based in China. TikTok Ireland infringed Article 13(1)(f) by failing to do so.

597. By reason of the failure of the October 2021 EEA Privacy Policy to provide the information outlined above, the DPC finds that TikTok Ireland infringed Article 13(1)(f) GDPR.

b) TikTok Ireland's December 2022 EEA Privacy Policy

598. TikTok Ireland further updated its EEA Privacy Policy during the course of the Inquiry, which it provided to the DPC under cover of its letter dated 26 October 2022.

599. TikTok Ireland advised that it intended that users would be notified of the updated Privacy Policy on 28 October 2022 through an in-app pop-up containing a hyperlink to the updated policy, and that the update to the Privacy Policy would take effect from 27 November 2022. TikTok Ireland subsequently informed the DPC that the update had taken effect from 2 December 2022.

600. The relevant sections of the updated December 2022 EEA Privacy Policy provided to the DPC were as follows (with hyperlinked content underlined):

> Our Global Operations and Data Transfers
>
> To support our global operations:
>
> We store the information described in What Information We Collect in secure servers located in the United States and Singapore.
>
> Certain entities in our Corporate Group located outside your country of residence (see here) are given limited remote access to this information so they can provide certain functions, as described in the Our Corporate Group section in How We Share Your Information. This access is limited, secure and only granted where necessary under strict security controls and authorisation approval protocols.
>
> We share What Information We Collect with service providers, partners and other third party entities, as described in How We Share Your Information. These third parties can be located outside your country of residence.
>
> These entities commit to processing 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 EEA, the UK, or Switzerland, we ensure it benefits from an adequate level of data protection by relying on:
>
> Adequacy decisions. These are decisions from the European Commission under Article 45 GDPR (or equivalent decisions under other laws) where they recognise that a country offers an adequate level

of data protection. We transfer your information as described in What Information We Collect to some countries with adequacy decisions, such as the countries listed here; or

Standard contractual clauses. The European Commission has approved contractual clauses under Article 46 of the GDPR that allows companies in the EEA to transfer data outside the EEA. These (and their approved equivalent for the UK and Switzerland) are called standard contractual clauses. We rely on standard contractual clauses to transfer information as described in What Information We Collect to certain entities in our Corporate Group (as described here) and third parties in countries without an adequacy decision.

For a copy of these adequacy decisions or standard contractual clauses, please contact us via the details provided in the Contact us section below.

601. Users who click on the hyperlinked word *"here"* in the second last paragraph of the extract quoted above should be brought to the following flyout:

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.

602. TikTok Ireland submitted in respect of the updated Privacy Policy dated 2 December 2022 that *"the update to the TikTok Privacy Policy provides even higher levels of transparency which go beyond the requirements of Article 13(1)(f) GDPR, and complement the protections offered to data subjects by the 2021 SCCs".*[261]

603. As appears from the passage quoted immediately above, the December 2022 EEA Privacy Policy did identify the third countries to which EEA user data was transferred, and did so in a manner which informed EEA Users which of those third countries have the benefit of an adequacy decision, and to which of the third countries TikTok Ireland transferred data pursuant to SCCs.

[261] TikTok Ireland's Submission dated 19 December 2022, at page 25

604. The December 2022 EEA Privacy Policy also informed EEA Users that personal data was stored on servers in the United States and Singapore, and was the subject of limited remote access by entities in TikTok's corporate group located in Brazil, China, Malaysia, Philippines, Singapore, and the United States.

605. The DPC acknowledges that a controller must balance the need to provide sufficient information in a privacy policy to enable users to have a clear understanding of, and insight into, the processing of their personal data, and the need to do so in a manner that is intelligible and accessible to all users. In this regard, the Article 29 Working Party has opined that the requirement for provision of information to data subjects to be done in a *"concise and transparent"* manner means that data controllers should present the information efficiently and succinctly in order to avoid information fatigue. Further, the requirement that information is *"intelligible"* means that it should be understood by an average member of the intended audience, with the use of clear and plain language.[262]

606. Arising from the above, the DPC has assessed TikTok Ireland's December 2022 EEA Privacy Policy as compliant with the requirements of Article 13(1)(f) GDPR in terms of the Data Transfers subject to the material scope of this Decision. For the avoidance of doubt, this Decision does not consider or make any findings regarding that Privacy Policy's compliance with Article 13(1)(f) GDPR in terms of the transfers that resulted in EEA User Data being stored on servers in China.

c) Finding in respect of Issue 5

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.

K. Finding of Infringement 2

608. Therefore, the DPC finds that TikTok Ireland infringed Article 13(1)(f) GDPR from 29 July 2020 to 1 December 2022 by failing to provide data subjects with required information on the Data Transfers and information on how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China.

[262] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP 260 (11 April 2018), at page 7.

L. Corrective Powers

609. As detailed above, the DPC has found that TikTok Ireland infringed the GDPR as follows:

(i) The DPC finds that, during the temporal scope of the Inquiry, TikTok Ireland infringed Article 46(1) GDPR by carrying out the Data Transfers while failing to verify, guarantee and demonstrate that 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.

(ii) The DPC finds that TikTok Ireland infringed Article 13(1)(f) GDPR from 29 July 2020 to 1 December 2022 by failing to provide data subjects with required information on the Data Transfers and information on how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China.

610. Under section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which corrective powers.

611. Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor. In deciding whether to exercise those powers, Recital 129 provides guidance as follows:

> …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…

612. Having carefully considered the infringements identified in this Decision, the DPC has decided to exercise certain corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) of the GDPR. In summary, the corrective powers that the DPC has decided are appropriate to address the infringements in the particular circumstances are:

(i) An order pursuant to Article 58(2)(j) GDPR requiring TikTok Ireland to suspend the Data Transfers.

(ii) An order pursuant to Article 58(2)(d) GDPR requiring TikTok Ireland to bring the processing into compliance in the manner detailed below.

(iii) Two administrative fines pursuant to Article 58(2)(i) GDPR in the amount of €485 million and €45 million respectively.

613. This Decision sets out further detail below in respect of each of these corrective powers and the reasons why the DPC has decided to exercise them.

M. Suspension of Data Flows pursuant to Article 58(2)(j) GDPR

614. The DPC finds that it is appropriate, necessary and proportionate to order the suspension of the Data Transfers pursuant to Article 58(2)(j) GDPR.

615. The DPC has set out above its finding that, in making the Data Transfers, TikTok Ireland infringed Article 46(1) GDPR. Therefore, the DPC must select corrective measures that are appropriate and necessary to ensure compliance with the GDPR, but which are also proportionate to that infringement.

616. In selecting corrective measures that are appropriate, necessary and proportionate, the DPC, in particular, has carefully considered the changes made by TikTok Ireland to the Data Transfers since the commencement of the Inquiry (including the changes made after the conclusion of the temporal scope of the Inquiry on 17 May 2023). This Decision sets out below why an order pursuant to Article 58(2)(j) is required.

a) Changes made to the Data Transfers after the Preliminary Draft Decision

617. TikTok Ireland submitted in its submissions on the Preliminary Draft Decision that, without prejudice to its position that the Data Transfers are complaint with Chapter V of the GDPR, even if this is not the case, the order suspending the data flows should not be made. In this regard, TikTok Ireland submitted that it is incumbent on the DPC to consider ongoing changes to how the Data Transfers operate (these changes relate to changes made by Project Clover and changes made by what TikTok Ireland termed the new measures). TikTok Ireland submitted that a suspension order would be disproportionate and unnecessary without first assessing whether the Data Transfers will be compatible with Article 46 GDPR once Project Clover has been fully implemented. TikTok Ireland submitted that the changes brought by Project Clover '*effectively neutralises the already remote risk that a public authority in China may seek to compel the China Group Entities or their employees to access EEA User Data stored outside of China…'*. TikTok Ireland also submitted that '*There is simply no doubt that, once Project Clover has been fully implemented, the EEA User Data will be subject to appropriate safeguards.'* TikTok Ireland provided its latest update on Project Clover on 11 April 2025.

618. TikTok Ireland's Project Clover Technical Report described the project's key goals as follows:

i. Data localisation: [redacted]

ii. Access controls: [redacted]

iii. Minimise data flows: [redacted]

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 [redacted][263]

619. TikTok Ireland's submissions in response to the Preliminary Draft Decision set out the effect of Project Clover as follows:

1) [redacted] in the European Enclave will not be accessible by China Group Entities or their employees [redacted]

2) China Group Entities will only have access to [redacted] in the Global Data Centres;

[redacted]

[263]Project Clover Technical Report, dated September 2023, at page 6.

4[redacted]

620. The DPC has carefully considered all information submitted by TikTok Ireland regarding the new measures and Project Clover. The DPC accepts that TikTok Ireland has made significant changes to the manner in which TikTok Ireland implements the Data Transfers. This Decision summarises below the key changes regarding the manner in which TikTok Ireland implements the Data Transfers.

i. Storage on servers of personal data of EEA users following changes implemented by TikTok Ireland after the Preliminary Draft Decision

621. Regarding EEA User Data created or received on or after 31 July 2023, TikTok Ireland informed the Inquiry that it stores that personal data in a data storage environment termed *"the European Enclave"*, [redacted] The Final European Enclave is hosted in three data centre environments in Ireland and Norway. [redacted]

622. Regarding the storage of EEA User Data on servers in China that TikTok Ireland notified the DPC of on 11 April 2025, the DPC notes for transparency purposes that TikTok Ireland contends that all such data was deleted from China on 26 March 2025. As noted above, the DPC will engage further with TikTok Ireland in relation to these matters which do not form part of the current Decision.

ii. Remote access by personnel of the China Group Entities following changes implemented by TikTok Ireland after the Preliminary Draft Decision

623. As a result of Project Clover, TikTok Ireland began distinguishing between EEA User Data that it defines as *"Protected Data"* and EEA User Data that it defines as *"Allowable Data"* (also known as *"Excepted Data"*). TikTok Ireland considers Allowable Data to be typically less confidential than Protected Data. Allowable Data consists of what TikTok Ireland describes as Public Data, Interoperable Data, and Aggregated Data:

> a) Public Data: This is EEA User Data that is publicly available on the TikTok platform (such as videos set to "Everyone" by the relevant EEA User)…

[264] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at pages 112 and 113.

b) Interoperable Data: This is EEA User Data which is necessary to enable global interoperability of the TikTok Platform (for example, where an EEA User wants to block a non-EEA User)…

c) Aggregated Data: EEA User Data that has been aggregated and/or anonymised for internal reporting or analysis.[265]

624. [redacted]

625. [redacted]

626. [redacted]

627. [redacted]

iii. Purposes for which the personal data is remotely accessed following changes implemented by TikTok Ireland after the Preliminary Draft Decision

628. The Data Transfer Assessment dated July 2024 refers to the purposes of processing as follows:

The China Group Entities provide various services in connection with the operation of Platform and are granted remote access for the following purposes:

- *Content delivery*
- *Customer and technical support*
- *Security*
- *Research and development*
- *Analytics*

[265] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at page 38.

● *Online payments*

● *Content moderation*

The China Group Entities are members of the corporate group of which TikTok forms part.

The remote access is limited to Authorised Remote Access to EEA User Data stored on servers in the US, Singapore and Malaysia (the "Global Data Centres").

Only personnel working for the China Group Entities who have been granted an approval are able to get Remote Authorised Access to the remotely accessible EEA User Data.

629. The Data Transfer Assessment dated July 2024 also refers to the nature of the processing as follows:

The nature of the processing is:

● Troubleshooting using engineering de-identified metrics or logs related to a specific user or, where necessary to fix the problem, deidentified specific user data.

● Fixing issues in the production system and validating that the issue has been successfully remediated.

● Viewing aggregated A/B testing results.

● Testing new tools, platforms and systems to ensure they work

correctly in a live environment.

● Analysing certain de-identified data such as reported user cases, account information, device information, behaviour logs, payment & transaction information to identify suspicious and malicious behaviours and building preventative models and tooling to combat these behaviours on the Platform.

● Developing, testing, maintaining and optimising machine learning models and algorithms.

● Reviewing de-identified customer feedback tickets to understand nature of specific technical issues, triaging these issues, routing to the appropriate engineering (or payment) team if necessary.

● Analysing aggregated business or technical metrics such as daily active users, daily new users, user growth, product feature engagement, and ads engagement.

● Supporting regional teams with creator development on a de-identified basis.

● Building aggregated dashboards for business teams.

● To protect the Platform from fraudulent payments, deal with chargeback queries from merchant banks and for financial regulation compliance purposes on a de-identified basis.

● Monitoring and evaluating content trends to ensure the effectiveness of Trust & Safety tools and strategies.

● Investigating de-identified moderation outputs in suspected cases of nmoderator misconduct.

● Reviewing of de-identified moderation outputs to determine how overall efficiency and effectiveness can be improved, and for capacity planning and training purposes.

iv. Categories of personal data the subject of remote access following changes implemented by TikTok Ireland after the Preliminary Draft Decision

630. As set out above, as a result of Project Clover, Allowable Data is subject to remote access, while Protected Data is not. Allowable Data consists of Public Data, Interoperable Data and Aggregated Data.

631. TikTok Ireland submitted the following outline of the categories of the personal data that constitutes '*Public Data'* to the Inquiry[266]:

Domain	Data Type	Field Examples	Treatment for Authorised Employees in China
Account	Account Attribute	badge, blue V (verified) tag	[redacted]
Account	Account Attribute	rank, score	[redacted]
Account	Account Metrics	following count, follower count	[redacted]
Account Profile	In-App Name	account name, nickname, anchor name	[redacted]
Account Profile	Profile Bio	bio	[redacted]

[266] Annex A to TikTok Ireland's submission of 17 May 2024.

Account Profile	Profile Image	avatar, image	[redacted]
Account Profile	Third Party Profile	twitter handle, instagram handle, youtube channel	[redacted]
Notification	Notice	notice content, notice title, push text, push title, copyright notice, push status	[redacted]
Real Life Identifier & Info	Email	email (only when creators set for contact purpose)	[redacted]
Transaction & Balance	Image	product's image in public live room	[redacted]
Transaction & Balance	Metadata	diamond count	[redacted]
Transaction & Balance	Attribute	gift price	[redacted]
Transaction & Balance	Metrics of gifts received	combo count	[redacted]
Location	Country, region, or city (when user chooses to add this using POI feature)	city	[redacted]
UGC	LIVE Attribute	description of a LIVE event in public profile page	[redacted]
UGC	Video	video content, video description	[redacted]
UGC	Video Captions	caption text	[redacted]

UGC	Video title	media_title , audio_title	[redacted]
UGC	Music title	music title	[redacted]
UGC	Creation Material in Videos and LIVE	icon and name of a effect/sticker	[redacted]
UGC	Content	video title	[redacted]
UGC	Photos	photos	[redacted]
UGC	LIVE streaming	LIVE in a public LIVE room	[redacted]
UGC	Comment	comment text	[redacted]
UGC	Shoutout	shoutout description	[redacted]
UGC	Point of Interest	poi name	[redacted]
UGC	LIVE Q&A	question content, source question	[redacted]
UGC	Hashtag	hashtag name	[redacted]
UGC	LIVE Event information	Event advertisement teaser	[redacted]
UGC	Country or Region or City when users use Point of Interest feature	country, region, city name	[redacted]
UGC	Image	public video cover image, music cover image, LIVE room cover image	[redacted]

UGC	Metadata	audio duration	[redacted]
UGC	Video metrics	Video likes count, video share count, video comment count, video view count, music view count, sticker use count, hastag view count, count of registered users for Events, reply count, photo like count, photo share count, LIVE room follow count, LIVE room like count, LIVE room share count, LIVE room shorward count, award count	[redacted]
UGC	Video permission	video permission status (for download, stitch and duet purposes)	[redacted]
UGC	Timestamp	comment post time, LIVE Event start timestamp	[redacted]
UGC	Public video playlist	video list of public playlist	[redacted]
User Behaviour Data	Content interaction events	donation description, name of the game played in a LIVE, images from the game played in the LIVE, goals of the LIVE	[redacted]

User Behaviour Data	Image	LIVE room icon	[redacted]
User Behaviour Data	Real Currency	amount of donation, shoutout earned	[redacted]
User Behaviour Data	LIVE Attribute	icon when user likes an anchor, diamond score	[redacted]
User Behaviour Data	Timestamp	donation create time, send gift success time	[redacted]

632. TikTok Ireland submitted the following outline of the categories of the personal data that constitutes *"Interoperable Data"* to the Inquiry[267]:

Domain	Data Type	Field Examples	Treatment for Authorised Employees in China
Account Profile	Profile Bio	badge type, verification type, bio	[redacted]
Real Life Identifier & Info	Age Level	user age level	[redacted]
Account	In-App User Relation	Follow status to user, follow status of user	[redacted]

[267] Annex A to TikTok Ireland's submission of 17 May 2024.

Account	Permission Settings	private account, public account, super admin permissions for LIVE, are push notifications allowed	[redacted]
Account	Moderation Outcome	review conclusion, LevelTag, moderation stage, reason for failing moderation	[redacted]
Account	Account Status	active status, cancel status, verified status	[redacted]
In-App User Relation	Block-list status	block status	[redacted]
User Behaviour Data	User Behavioural Record	invite friend, delete message, pinned event, video play duration, count of videos played, share description, count of share.	[redacted]
User Behaviour Data	Timestamp	send time, create time, start and end time	[redacted]
User Behaviour Data	Conversation Attributes	conversation type (notification or chat), conversation enumeration	[redacted]
Notification	Push notice	notice content, notice title, push text, push title, copyright notice, push status	[redacted]

Location	Country, region, or city	region code, country code, reporter region, user store region code, moderation queue country code	[redacted]
Direct Message	Direct Message Content	message content	[redacted]
Direct Message	Direct Message Metadata	message type (text, emoji)	[redacted]
Direct Message	Direct Message Permission Settings	message permission, permission status	[redacted]
Direct Message	Direct Message Status	is read	[redacted]
Direct Message	Attribute	group name and icon, group description	[redacted]
First Party Identifier	Video ID	video id	[redacted]
First Party Identifier	User ID	user id, block status	[redacted]
First Party Identifier	Advertisement ID	ad id	[redacted]
First Party Identifier	Appeal ID (alleged copyright infringements)	appeal id	[redacted]
First Party Identifier	Comment ID	parent comment id, comment id	[redacted]
First Party Identifier	Direct Message ID	message id	[redacted]
First Party Identifier	LIVE ID	LIVE room id	[redacted]

First Party Identifier	Moderation ID	moderation task id, moderation outcome id	[redacted]
First Party Identifier	Other UGC ID	effect id, sticker id, emote id, audio id, music id	[redacted]
First Party Identifier	Photo ID	item id	[redacted]
First Party Identifier	Penalty ID	penalty id	[redacted]
First Party Identifier	Push & Notice ID	notice id	[redacted]
First Party Identifier	Phrase ID	user phrase id	[redacted]
First Party Identifier	Report ID	report id	[redacted]
First Party Identifier	Virtual Product ID	product id, gift id	[redacted]
First Party Identifier	Device ID (not linked to user id or other identifiers- used	device id	[redacted]
	with user region to route users to the correct TikTok Platform)		
First Party Identifier	Interaction IDs	event id, conversation id	[redacted]
UGC	Video	video content	[redacted]
UGC	URLs	account, video, photo, other UGC	[redacted]
UGC	Image / Photos	image content	[redacted]

UGC	Language	LIVE language, auto caption language, language code, video language	[redacted]
UGC	Content	captions, video title, subtitle, video description, comments, hashtag, search term, questions, LIVE room title	[redacted]
UGC	Metadata	font size, length, colour, video duration	[redacted]
UGC	Metrics	comment count, fans count, share count, follower count, play count, share count	[redacted]
UGC	Permission settings for comments, LIVE, photo, video		[redacted]
UGC	Moderation status of UGC	risk type, status before deletion, ban time, ban duration.	[redacted]
Account or Content Tag and Log	Model Feature	model result rate, task start time, model score	[redacted]
Account or Content Tag and Log	Model Attribute	model name, model version	[redacted]

User Support and User Requests	Report Reason	report reason, reporter region, report description, report start time	[redacted]
User Support and User Requests	Ban Record	ban begin time, expire time	[redacted]
User Support and User Requests	Penalty Status	penalty type, ban type	[redacted]

633. TikTok Ireland described *"Aggregated Data"* as EEA User Data that has been aggregated and/or anonymised for internal reporting or analysis. [redacted] in some cases it is still possible to gain information about specific users from aggregated data. TikTok Ireland implements [redacted] safeguards to de-identify aggregated results.

v. Format of personal data remotely accessed following changes implemented by TikTok Ireland after the Preliminary Draft Decision

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"*. [redacted]

vi. Further Supplementary measures implemented after the date of the Preliminary Draft Decision

635. In addition to the changes brought about by Project Clover, TikTok Ireland also implemented the additional supplementary measures. A significant number of these additional supplementary measures related to how employees from the China Group Entities access remotely accessible EEA User Data.

636. First, TikTok Ireland submitted that employees from the China Group Entities requesting access to systems containing EEA User Data must now submit a data authority application, which follows a defined approval workflow based on the sensitivity of the requested system or data. These requests must be approved by

TikTok's data protection security team. TikTok Ireland submitted during the Inquiry that this data authority application was required in respect of any access to Accessible Data

637. Second, TikTok Ireland submitted that employees from the China Group Entities who do not need sustained access to EEA User Data must instead request ad hoc permission, which must go through a multi-tiered approval process. Employees can request ad hoc access up to a maximum of [redacted] during a defined period (generally [redacted] from the date the original permission is granted). If the employee exhausts their allocation of ad hoc access permissions they must go through the full multi-tiered access request approval process again.

638. Third, TikTok now automatically revokes granted permissions for employees of the China Group Entities who do not use the permission in a [redacted].

639. Fourth, TikTok removed the ability for employees in the China Group Entities to request access to decrypt encrypted Legacy Protected Data in the Global Data Centres that is encrypted at rest within databases and its main applications in the Global Data Centres.

640. Fifth, employees of the China Group Entities no longer have access to encryption/decryption keys to EEA User Data. Instead, such keys are assigned only to employees who are located outside of China and who are not employed by the China Group Entities.

641. Sixth, TikTok Ireland submitted to the Inquiry that employees of the China Group Entities can no longer download or export EEA User Data in applications, which prevents downloaded or exported data from being stored locally on laptops.

642. Seventh, TikTok implements data loss prevention software on the laptops of employees in the China Group Entities who have access to EEA User Data. TikTok Ireland submitted that, as a result, security teams would be alerted if those employees shared data from their laptop to a third party via website, email or USB.

643. Eighth, TikTok has implemented an internal threat monitoring programme to detect suspicious behaviours within its systems, applications and databases. TikTok Ireland submitted that security teams are now alerted if such behaviours are detected.

644. TikTok Ireland's position is that the supplementary measures that it implemented before Project Clover were appropriate to protect EEA User Data to a standard that is essentially equivalent with EU law. Nonetheless, TikTok Ireland's submissions in response to the Preliminary Draft Decision emphasised the further steps it has taken to implement new measures as part of Project Clover. TikTok Ireland submitted that these new measures fully address the concerns articulated in the Preliminary Draft Decision.

b) Data Transfer Assessments after the Preliminary Draft Decision

645. As set out above, TikTok Ireland submitted 5 Data Transfer Assessments as part of its various sets of submissions made during the Inquiry. The *"October 2023"* and *"July 2024"* Data Transfer Assessments postdate the temporal scope of the Inquiry. As set out above, the DPC has considered these assessments insofar as they provide additional information to support the conclusions in TikTok Ireland's 2021 and 2022 assessments, in particular TikTok Ireland's conclusion that the Data Transfers fall outside the territorial scope of the Problematic Laws.

646. The DPC has also had particular regard to the 2023 and 2024 assessments in considering whether it is appropriate, necessary and proportionate to order the suspension of the data flows and to order TikTok Ireland to bring its processing into compliance.

647. TikTok Ireland's 2023 and 2024 Data Transfer Assessments made updates to account for a number of changes. The Assessments reflect how TikTok Ireland stores EEA User Data created or received after [redacted] in

the European Enclave and how it implemented measures to limit remote access [redacted] These Data Transfer Assessments did not consider the EEA User Data that was stored on servers in China in circumstances where TikTok Ireland now states that it was not aware of that storage when the assessments were made.

648. In the 2023 and 2024 Assessments, TikTok Ireland applied its assessment of Chinese law and practices to provide an equivalency assessment for two distinct types of transfers: (1) direct transmission to servers in China based on SCCs alone, and (2) transfers by remote access to data stored outside China. According to TikTok Ireland, this resulted in it being able to conclude on the effectiveness of the remote authorised access transfer mechanism in Section 2 of its Assessment, rather than Section 3 as was the case in the 2021 and 2022 Assessments. As a result, its overall summary of assessment in respect of transfers under the 2021 SCCs was updated in the 2023 and 2024 Assessment as follows:

> Based on the assessment of China's current legal framework, it provides for: (1) binding applicable data protection laws (although they may not be entirely equivalent to EU standards); (2) rules circumscribing surveillance powers, including requirements for ex ante authorisation; (3) surveillance regimes that are subject to legality and proportionality requirements; (4) administrative oversight; (5) various authorities authorised to enforce the data protection laws, with the Cyberspace Administration of China being tasked to lead and coordinate the enforcement activities among the ministries; and (6) rights of individual redress against abuses of power and unlawful surveillance and in relation to breaches of data protection laws more generally.
>
> The assessment also demonstrates that Chinese authorities must rely on bilateral and/or multilateral assistance mechanisms with other jurisdictions or other diplomatic channels to request access to data stored outside of China for evidence collection in law enforcement or judicial proceedings (including crimes related to national security).
>
> For the reasons explained below, the conclusion has been reached that:
>
> (1) There are aspects of the current legal framework that preclude a finding of essential equivalence to the EU standard in circumstances where there is a direct transmission to servers in China based on SCCs alone. In this regard, TikTok and each China Group Entity accepts that SCCs alone cannot provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law.
>
> (2) The current legal framework provides an essentially equivalent level of protection in circumstances where the transfer takes place by way of remote access to data stored outside China.
>
> 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 described in Section 3 below which provide for the transfers to take place by way of remote access to data stored outside China.[268]

649. This Decision sets out below the key changes made by the TikTok Ireland's 2023 and 2024 Data Transfer Assessments as compared to the assessments relevant to the temporal scope.

[268] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 19.

i. Regulation of data privacy

650. TikTok Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding direct transmissions of data to servers in China, Chinese law and practices provides a high level of safeguards, but diverges from EU standards.

651. TikTok Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding remote access, Chinese law and practices offered a high level of safeguards, essentially equivalent to the EU.

652. Section 2.1 of the 2023 and 2024 Assessments also refer to the Legislative Affairs Commission of the National People's Congress interpretation of the Constitution that the right to freedom and privacy of correspondence is a critical constitutional right and that the core of the right to freedom and privacy of correspondence is to protect the right to privacy. Article 32 of the PRC Constitution provides that it protects the rights and interests of foreigners. While, Article 38 of the PRC Constitution provides for the right to personal dignity, which the Legislative Affairs Commission of the National People's Congress has confirmed that this encompasses, among other rights, the right to privacy.

653. When considering the prospect of transfers by means of direct transmission to servers in China, TikTok Ireland's 2024 Assessment concludes in respect of the safeguards provided by Chinese law relevant to Essential Guarantee A:

> However, these safeguards are not essentially equivalent to those required under European Essential Guarantee A and do diverge from them. For instance, the criteria for granting approval to a Chinese authority exercising its powers under the laws described in Section 2.2B tend not to be published and some of the laws themselves (similar to a number of laws in the EU) may not include a clear definition of the scope of the limitation on the exercise of the right concerned, in what circumstances and under which conditions the measure may be adopted or the minimum safeguards to the extent required by European Essential Guarantee A. By way of example, Article 4 of the Counter-Espionage Law confers certain powers on state security authorities to conduct counter-espionage work, but does not exhaustively define what constitutes "espionage conduct" but instead retains a catch all reference to "conducting other espionage activities" as an example of "espionage conduct". As a further example, whilst the Criminal Law sets out quite detailed rules regarding the use of technical investigative measures, they are not as clear and precise when it comes to requests for disclosure of data other than pursuant to technical investigative measures.[269]

654. TikTok Ireland's 2024 Assessment concludes that the divergence from European Essential Guarantee A identified in those assessments does not result in a lack of essentially equivalent protection in respect of transfers made by way of remote access. The basis for TikTok Ireland's conclusion is that *"Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China".*[270]

[269] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 22.
[270] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 23.

ii. Regulation of public authority access to personal data in China

655. TikTok Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding direct transmissions of data to servers in China, Chinese law and practices provide some safeguards, but materially diverges from EU standards.

656. TikTok's 2023 and 2024 Data Transfer Assessments concluded that, regarding remote access, Chinese law and practices provide a high level of safeguards, essentially equivalent to the EU.

657. TikTok Ireland's 2024 Assessment concludes that the divergence from European Essential Guarantee B identified in that assessment does not result in a lack of essentially equivalent protection in respect of transfers made by way of remote access. The basis for TikTok Ireland's conclusion is that *"Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China".*[271]

iii. Regulatory supervision

658. TikTok Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding direct transmissions of data to servers in China, Chinese law and practices provide some safeguards, but materially diverges from EU standards.

659. TikTok's Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding remote access, Chinese law and practices provide a high level of safeguards, essentially equivalent to the EU.

660. TikTok Ireland's 2023 and 2024 Assessments set out the role of the People's Procuratorates specifically in instituting public interest lawsuits on behalf of individuals whose rights to personal information protection have been violated by public authorities, and their role in supervising criminal investigations and proceedings (including evidence collection activities for national security related criminal investigations). Furthermore, the assessments set out People Procuratorates' supervision over civil proceedings, administrative authorities and administrative proceedings, their instigation of public interest litigation including in respect of personal information protection rights. The assessments also detailed how internal oversight is implemented within authorities regarding their access to privately-held data, including by means of required approval at senior levels or a separate department within the authority, internal procedures and policies, establishment of internal audit or supervisory departments, conducting scheduled and unscheduled reviews and examinations, conducting internal investigations and imposing disciplinary sanctions on staff where appropriate. The assessments also detailed how this access is also subject to internal oversight by upper level authorities, which includes supervisory powers to oversee, review and correct decisions taken at lower levels of the authority. The oversight power of upper level authorities can be exercised through various means, including: (i) ex-ante approval process from a superior authority before taking specific measures authority at the upper level; (ii) legal review of the normative documents adopted by lower level authority in accordance with the procedures set forth under the Legislation Law; (iii) implementing reviews and investigations over the measures taken by lower authorities, (iv) reviewing the lower authorities' acts in the administrative reconsideration procedure in accordance with the PRC Administrative Reconsideration Law; (v) requesting lower authority to make corrections, and (vi) pursuing responsibility and imposing disciplinary penalties against the lower level authorities. When an individual or organisation, such as a data subject or China Group Entity, thinks that the public security authority or national security authority infringed his or her legal rights

[271] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 41.

in criminal proceedings or collected evidence by illegal methods, the individual has the right to report it to the People's Procuratorate or file a complaint.

661. TikTok Ireland's 2024 Assessment concluded that the divergence from European Essential Guarantee C identified in those assessments do not result in a lack of essentially equivalent protection in respect of transfers made by way of remote access. The basis for TikTok Ireland's conclusion is that *"Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China".*[272]

iv. Rights of redress

662. TikTok Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding direct transmissions of data to servers in China, Chinese law and practices provide a high level of safeguards, but diverges from EU standards.

663. TikTok's 2023 and 2024 Data Transfer Assessments concluded that, regarding remote access, Chinese law and practices provide a high level of safeguards, essentially equivalent to the EU.

664. In particular, TikTok Ireland's 2023 and 2024 Assessments concluded that the divergence from European Essential Guarantee D identified in that assessment does not result in a lack of essentially equivalent protection in respect of transfers made by way of remote access. The basis for TikTok Ireland's conclusion is that *"Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China".*[273]

v. International treaties

665. TikTok Ireland's 2023 and 2024 Data Transfer Assessments concluded that, regarding direct transmissions of data to servers in China, China provides some safeguards, but materially diverges from EU standards.

666. TikTok's 2023 and 2024 Data Transfer Assessments concluded that, regarding remote access, China provides a high level of safeguards, essentially equivalent to the EU.

667. TikTok Ireland's 2023 and 2024 Assessments stated:

> China is not a party to any treaties to which the US, Singapore and Malaysia are a party that would provide Chinese authorities with a right to directly access data stored outside China.[274]

668. TikTok Ireland's 2024 Assessment concludes that the divergence identified in Section 2.5 of its assessments do not result in a lack of essentially equivalent protection in respect of transfers made by way of remote access. The basis for TikTok Ireland's conclusion is that *"Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China".*[275]

---

[272] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 83.
[273] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 100.
[274] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 111.
[275] TikTok Ireland's Data Transfer Assessment, dated July 2024, at page 111.

vi. Outcome of assessments

669. The outcome of TikTok Ireland's Data Transfers Assessments at Section 2 differ between the 2021 & 2022 Assessments as compared to the 2023 & 2024 Assessments in respect of the conclusion in this section as to whether Chinese law and practices provide a level of protection essentially equivalent to the EU. All of the assessments acknowledge that the legal framework in China has issues that would preclude a finding of essential equivalence to EU law, even where SCCs are used. However, in the 2023 and 2024 Assessments, TikTok Ireland applied its assessment of Chinese law and practice to provide an equivalency assessment for both transfers by means of direct transmission to servers in China based on SCCs alone, and for transfers by remote access to data stored outside China. TikTok Ireland's conclusion at Section 2 of the 2023 and 2024 Data Transfer Assessments (as opposed to Section 3 in the 2021 & 2022 Assessments) is that the adopted form of transfer mechanism effectively ensures that the transferred data will be afforded a level of protection in China that is essentially equivalent to that guaranteed in the EU.

670. TikTok Ireland stated in its 2023 and 2024 Assessments that this conclusion is contingent on the transfers being implemented by way of remote access to EEA User Data stored outside China and it recommended that appropriate supplementary measures for this are implemented accordingly. Section 3 of the 2023 and 2024 Assessments consider the Supplementary Measures. TikTok Ireland described the Supplementary Measures outlined in Section 3 of the 2023 and 2024 Assessments as ensuring that the transfers to the China Group Entities are implemented by way of remote access to EEA User Data stored on servers outside China. Having concluded in Section 2 of the 2023 and 2024 Assessments that the current legal framework provides an essentially equivalent level of protection, TikTok Ireland states that this conclusion is contingent on TikTok having implemented the necessary supplementary measures to ensure the transfers take place only by way of remote access to data stored outside China.

671. While there are differences between the 2021 & 2022 Assessments as compared to the 2023 & 2024 Assessments, the conclusion in all assessments, that the divergences in Chinese law and practices do not result in a lack of essentially equivalent protection if the transfers are made by means of remote access to data stored outside China, places the same reliance on the territoriality principle. Having identified divergences from the European Essential Guarantees, the conclusions in sections 2.1, 2.2, 2.3, 2.4, and 2.5 of the 2023 and 2024 Assessments regarding how the divergences identified do not result in a lack of essentially equivalent protection relies on the following position that is repeated in each section:

> Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China.[276]

c) Conclusion on suspension order

672. Having considered the changes made by TikTok Ireland since the end of the temporal scope of the inquiry, the DPC finds that it is appropriate, necessary and proportionate to order the suspension of the Data Transfers pursuant to Article 58(2)(j) GDPR. The DPC finds that the only corrective measures that are adequate to achieve the objective of ensuring compliance with the GDPR following an infringement of Article 46 GDPR are the banning or suspension of the Data Transfers. In order for TikTok Ireland to rely on Article 46 for the Data Transfers, it was first obliged to verify and guarantee an essentially equivalent level of protection. Its failure to do so mandated that TikTok Ireland, or failing that, the DPC, suspend or end the transfers. Accordingly, an

[276] TikTok Ireland's Data Transfer Assessment, dated October 2023, at pages 21, 41, 78, 93, and 103. TikTok Ireland's Data Transfer Assessment, dated July 2024, at pages 23, 41, 83, 100 and 111.

order requiring the suspension of the Data Transfers is the least onerous measure that ensures compliance with the GDPR.

673. This order provides for the situation whereby, if measures become available to make the Data Transfers compliant, then the suspension could be re-considered. The DPC is not imposing a permanent ban on the Data Transfers, recognising that new measures, not currently in operation, may yet be capable of being developed and implemented by TikTok Ireland to compensate for the deficiencies identified in this Decision. If that situation were to arise, the DPC would then be in a position to reconsider the suspension. Therefore, the suspension is a proportionate response in all the circumstances. As set out in this Decision, the obligation rests with TikTok Ireland to verify, guarantee and demonstrate that the transferred personal data will be afforded a level of protection essentially equivalent to that guaranteed within the European Union in order to make transfers pursuant to Article 46 GDPR. If, in the future, TikTok Ireland is in a position to do so, the DPC can reconsider the suspension. Furthermore, while the DPC has found above that the derogations referenced by TikTok Ireland cannot be relied upon in respect of the Data Transfers made during the temporal scope, which, as set out above, were systematic, repetitive, and continuous. If TikTok Ireland can demonstrate that specific derogations are applicable to proposed specific transfers, for example, by demonstrating how valid consent can be obtained, or by producing the assessment required by the second subparagraph of Article 49(1), the DPC can reconsider the suspension.

674. Given the circumstances of the Data Transfers and all of the other factors outlined above, a suspension of data transfers is appropriate and proportionate. It is appropriate that the Data Transfers be suspended pursuant to the DPC's powers under Article 58(2)(j) GDPR. This suspension order will take effect in accordance with the timeline specified below.

675. The responsibility to ensure that data transfers are only made in circumstances in which a level of protection is ensured that is essentially equivalent to that provided by the GDPR, read in light of the Charter, falls in the first instance on the EU controller or processor. In the Schrems II judgment, the CJEU held that this requires the controller or processor to verify, on a case-by-case basis, whether the law of the third country ensures essential equivalence. The CJEU has also held that if that controller or processor is not able to guarantee such protection by means of additional measures, that controller or processor is required to suspend or end the transfer.

676. However, the CJEU was also clear that this obligation to suspend or end the transfer falls on the competent supervisory authority where the controller or processor has failed to suspend or end the transfer.

677. The DPC has found that TikTok Ireland has failed to verify, guarantee and demonstrate that the supplementary measures and the SCCs were effective to ensure that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within the EU.

678. The DPC finds that an order suspending the data flows is necessary but no more than necessary in order to ensure compliance with the GDPR. The DPC is satisfied that this order is necessary to remedy the infringement of Article 46(1). This corrective power is appropriate, necessary and proportionate in order to end the unlawful data transfers.

679. The CJEU stated in the Schrems II judgment that supervisory authorities should suspend any data transfer if *"in light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be*

complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means".[277]

680. The DPC is satisfied that this requirement to suspend data transfers applies equally to circumstances in which the controller or processor has failed to verify whether the law of the third country ensures an essentially equivalent level of protection in the context of the transfers and in light of the safeguards and supplementary measures implemented and, therefore, has failed to guarantee and demonstrate such protection. TikTok Ireland disputed this in its submissions on the Preliminary Draft Decision. According to TikTok Ireland, a suspension order would be appropriate only if the DPC formed the view that there are no alternative means that enable the EEA User Data to be adequately protected.

681. The DPC does not accept this submission. The structure of Chapter V of the GDPR is clear that it places the obligation on the controller or processor to first verify that personal data transferred to a third country will be afforded a level of protection essentially equivalent to that guaranteed within the European Union. Fundamentally, it is for the controller or processor to identify and implement measures to adequately protect the data. The controller or processor established in the European Union must guarantee such protection in light of the additional measures. The Schrems II judgment is clear that the controller or processor must suspend or end the transfers if it is not able to take adequate additional measures to guarantee that level of protection. If the controller or processor has failed to verify and guarantee an essentially equivalent level of protection, it is required to suspend or end the transfer. The Schrems II judgment also 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 do so. This Decision has set out above how the obligation on controllers or processors to verify and guarantee that transfers made under Article 46 GDPR are subject to a level of protection essentially equivalent to that which is guaranteed in the European Union is crucial to upholding the fundamental rights of data subjects, particularly in circumstances where when personal data moves across borders, there is a particular risk that the level of protection can be undermined. The DPC finds that, in circumstances where TikTok Ireland has failed to verify and guarantee that EEA User Data transferred to China is afforded a level of protection essentially equivalent to that guaranteed within the European Union, it is appropriate, necessary and proportionate for the DPC to order the suspension of the Data Transfers.

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.

683. The DPC has carefully considered the changes made by TikTok Ireland to the Data Transfers after the Inquiry commenced, including all information submitted regarding the changes made after the temporal scope of the Inquiry. Having regard to this information, the DPC finds that TikTok Ireland, on an ongoing basis, has failed to demonstrate that it has verified and guaranteed that EEA User Data transferred to China is afforded a level of protection essentially equivalent to that guaranteed within the European Union. For the reasons that follow, the DPC's concerns as set out in Issues 2, 3 and 4 of this Decision remain, notwithstanding the changes implemented by TikTok Ireland.

[277] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, judgment of 16 July 2020 (ECLI:EU:C:2020:559), paragraph 113.

684. TikTok Ireland has failed on a continuing basis to adequately assess the level of protection of EEA Users by Chinese law and practices under the Chinese legal framework in the context of the transfers. The DPC has carefully considered TikTok Ireland's latest Data Transfer Assessment, dated July 2024. In arguing that there is essentially equivalent protection in respect of transfers made by way of remote access, the TikTok Ireland Assessment repeatedly relies on the statement that:

> Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China.[278]

685. TikTok Ireland's assessment of Chinese law and practices has overlooked how the territoriality principle applies in respect of EEA User Data that is processed in China. While Project Clover resulted in significant changes to the manner in which the Data Transfers are implemented, it has not changed the fact that the Data Transfers on an ongoing basis entail the processing of EEA User Data on computer information systems in China. The Data Transfers, even after the changes made by Project Clover, are still subject to remote access by the China Group Entities. Therefore, the DPC's concerns regarding TikTok Ireland's analysis of the territoriality principle in the context of the Data Transfers, as set out in this Decision, remain in the context of the ongoing Data Transfers. As a result, the DPC finds that TikTok Ireland has continually failed to establish that the territoriality principle does in fact operate so as to prevent the application of problematic laws in practice to the ongoing Data Transfers.

686. TikTok Ireland has also failed on an ongoing basis to set out in a clear way the deficiencies it acknowledges to exist in the Chinese legal framework. Its analysis of Chinese law and practice does not set out in a clear way these deficiencies and the resulting risk in respect of the specific processing of EEA User Data subject to the Data Transfers. Its July 2024 Data Transfer Assessment, while acknowledging a lack of equivalence of Chinese law with that of EU law regarding direct transmissions of data to servers in China, failed to provide sufficient consideration to how those divergences could apply to EEA User Data subject to the Data Transfers in the context of how those transfers involve processing of EEA User Data in China by means of the Remote Access Solution. By failing on an ongoing basis to adequately define the scope of the divergences, TikTok Ireland failed to address how those divergences could impact EEA User Data that is processed in China. As a result, TikTok Ireland has continually failed to adequately assess the law and practices in effect in China in the context of the ongoing Data Transfers and the level of protection that is provided to the personal data of EEA Users. In light of TikTok Ireland's ongoing failure to appropriately consider how the territoriality principle applies in respect of the Data Transfers, and its ongoing failure to set out the deficiencies that it acknowledges to exist in the Chinese legal framework, the DPC finds that TikTok Ireland has, on a continuing basis, failed to adequately assess the level of protection provided to EEA User data by Chinese law and practices in the context of the ongoing Data Transfers.

687. TikTok Ireland's ongoing failure to adequately assess the level of protection provided by Chinese law and practices prevents it from demonstrating that the law and practices in China do not undermine the effectiveness of the SCCs and supplementary measures in ensuring an essentially equivalent level of protection. TikTok Ireland's failure to assess, in light of the Data Transfers, the deficiencies in the protection afforded in China that it acknowledges to exist means that it is not in a position to demonstrate that its supplementary measures guarantee an essentially equivalent level of protection and that yet further supplementary measures are not required to address the identified divergences. Furthermore, TikTok

[278] TikTok Ireland's Data Transfer Assessment, dated July 2024, at pages 23, 41, 83, 100, and 111.

Ireland's failure to appropriately consider how the territoriality principle applies in the specific context of the Data Transfers has prevented it from demonstrating that the transferred EEA User Data is subject to an essentially equivalent level of protection. In circumstances where the deficiencies have not been clearly established, it is not possible for TikTok Ireland to subsequently demonstrate that an essentially equivalent level of protection has been achieved. Therefore, TikTok Ireland's failure to adequately assess the level of protection provided by Chinese law and practices in the context of the Data Transfers not only directly impacts TikTok Ireland's ability to select appropriate safeguards and supplementary measures, but also prevents TikTok Ireland from demonstrating an essentially equivalent level of protection on an ongoing basis.

688. The DPC has carefully considered the additional supplementary measures implemented by TikTok Ireland after the temporal scope of the Inquiry. As a result of these changes, TikTok Ireland submitted that it limits the EEA User Data subject to the Data Transfers to what it terms Accessible Data. This resulted in a significant reduction in the categories of personal data subject to the Data Transfers. TikTok Ireland submitted that Protected Data is no longer subject to the Data Transfers. Irrespective, the categories of personal data subject to the Data Transfers on an ongoing basis are still extensive and on a continuing basis result in a broad range of categories of personal data being transferred to China by means of remote access. Further, TikTok Ireland has consistently denied that the problem of access to EEA User Data in China exists.

689. 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.

690. 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.

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 Xu 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.

692. TikTok Ireland submitted that the suspension order would be disproportionate having regard to the harm a suspension order would cause to TikTok, its users, content creators, and third party advertisers. TikTok Ireland has cited its freedom to conduct a business pursuant to Article 16 of the Charter. TikTok Ireland stated that the suspension order '*would mean that China Group Entities can no longer provide* [redacted] *services which require access to EEA User Data or to rest of world ("RoW") user data*'.

693. The DPC acknowledges that the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. The DPC also accepts that it is required to exercise any corrective power in a manner that is appropriate, necessary and proportionate, taking into account the circumstances of the individual case. However, for the reasons that follow, the DPC does not accept TikTok Ireland's submission that a suspension order would be disproportionate.

694. In the first instance, it is important to note that the analysis of whether Article 46 GDPR has been infringed is conducted within the framework of the GDPR and as such, insofar as appropriate, relevant fundamental rights are balanced accordingly. The DPC has found that TikTok Ireland infringed Article 46 GDPR and that determination is the product of, *inter alia*, a proportionality-based assessment embedded in the legislative scheme. The DPC finds that the requirement to reconcile the right to the protection of personal data with other fundamental rights is embedded into the scheme of the GDPR, rather than required as part of an assessment for the purposes of Article 58(2) GDPR.

695. What is required when considering the adoption of corrective measures under Article 58(2) GDPR is an assessment of what is "*appropriate, necessary and proportionate in view of ensuring compliance with*" the GDPR.[279] To conduct a further balancing of rights as suggested by TikTok Ireland would not be appropriate at this stage as it carries with it the possibility that an infringement of the GDPR would be permitted to continue, particularly an infringement causing continuing damage to EU/ EEA citizens. The assessment of whether there has been an infringement of the GDPR will have already taken place prior to consideration of the appropriate corrective measure. Under the proper legislative scheme, once the infringement has been established, it is for the supervisory authority to adopt those corrective measures (if any) which are appropriate and necessary to ensure compliance with the GDPR, but which are also proportionate to the relevant infringement.

696. The DPC finds that a suspension of the Data Transfers is necessary but no more than necessary in order to ensure compliance with the GDPR. The DPC is required to take appropriate action in order to remedy the infringement of Article 46 GDPR. The DPC finds that it is appropriate, necessary and proportionate to invoke the power under Article 58(2)(j) GDPR to order the suspension of the Data Transfers. The DPC acknowledges

[279] Recital 129 GDPR.

that, consistent with the requirement that any corrective measure be appropriate, necessary and proportionate, where "*there is a choice between several appropriate measures recourse must be had to the least onerous*".[280] It is important to note that the appropriateness of the relevant measures is determined by reference to the objective to be achieved. In this instance, the objective is to ensure compliance with the GDPR in circumstances where, in making the Data Transfers, TikTok Ireland has infringed Article 46 GDPR. The only corrective measures that are adequate to achieve the said objective are the banning or suspension of the Data Transfers. Accordingly, the suspension of the Data Transfers is the least onerous measure that ensures compliance with the GDPR. The DPC considers that a suspension order is more appropriate than a ban because, if measures become available to make the Data Transfers compliant, then the suspension could be re-considered. Therefore, a suspension is a proportionate response in all the circumstances.

697. As set out under Issue 4 of this Decision, TikTok Ireland did not rely on the Article 49 Derogations in respect of the Data Transfers up to and including the date upon which those submissions were made, 9 September 2023. However, TikTok Ireland submitted that it reserves its entitlement to rely on the derogations if the DPC finds that TikTok Ireland cannot lawfully transfer the personal data subject to the Data Transfers in reliance on Article 46 GDPR. Specifically, TikTok Ireland contended to the inquiry that it is entitled to rely on the derogations in respect of contractual necessity pursuant to Article 49(1)(b) GDPR and of compelling legitimate interests pursuant to the second subparagraph of Article 49(1) GDPR for certain of the transfers of EEA User Data. TikTok Ireland also stated that it reserved its entitlement to rely on consent in accordance with Article 49(1)(a).

698. The DPC has had regard to this contention when deciding to make this suspension order. As set out above, the Data Transfers ongoing during the temporal scope concerned systematic, repetitive, and continuous transfers of personal data to China. The Data Transfers cannot be considered occasional or not-repetitive. The DPC has carefully considered the changes made to the Data Transfers following the temporal scope, including the changes brought about by Project Clover. For the reasons set out above, the DPC finds that these transfers are also systematic, repetitive, and continuous, and cannot be considered occasional or not-repetitive.

699. In circumstances where these transfers are systematic, repetitive, and continuous in nature, the DPC's concerns set out at Issue 4 above regarding the consent derogation under Article 49(1)(a) GDPR remain. It is unclear how, on a practical level, TikTok Ireland could obtain valid consent for these systematic, repetitive, and continuous transfers in circumstances where a single consent by an EU/EEA data subject cannot justify any and all future transfers of that user's personal data to China, and a single consent cannot be obtained for ongoing data transfers and/or different sets of transfers.

700. The DPC's concerns regarding the contractual derogation under Article 49(1)(b) GDPR also remain. For the reasons set out above, Article 49(1)(b) GDPR can be relied on to justify occasional transfers only. As set out above, TikTok Ireland has also failed to demonstrate the necessity of the transfers. Therefore, the contractual necessity derogation cannot be relied on to justify the systematic, repetitive and continuous transfers to China within the Data Transfers.

701. The DPC's concerns regarding the derogation under the second subparagraph of Article 49(1), which requires a compelling legitimate interest also remain. As set out above, this derogation can be relied on to justify occasional transfers only. While the extent to which TikTok Ireland could rely on this derogation to justify any data transfers in the future cannot be determined in the abstract, and TikTok Ireland has not produced a

[280] Case C-311/18 *Fedesa*, paragraph 13.

balancing test between the data exporter's compelling legitimate interest pursued and the interests or rights and freedoms of the data subject, the DPC finds that this derogation cannot be relied upon for the systematic, repetitive and continuous transfers to China which are ongoing following the changes brought about by Project Clover.

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.

N. Order to bring processing into compliance pursuant to Article 58(2)(d) GDPR

703. The DPC finds that it is appropriate, necessary and proportionate to order TikTok Ireland to bring its processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing in China of EEA User Data transferred in violation of the GDPR. This order will take effect in accordance with the timeline specified below.

704. It is TikTok Ireland's responsibility to identify and implement the appropriate measures to bring processing of EEA User Data unlawfully transferred to China into compliance with the GDPR. This order does not impose a specific manner for TikTok Ireland to comply with it. Therefore, this order gives enough room of manoeuvre to TikTok Ireland to identify the most suitable manner to implement the order, in accordance with its accountability obligations. Therefore, this order is the least onerous measure possible and it does not create disproportionate disadvantages to the aim pursued. However, to comply with the order, TikTok Ireland must ensure that any EEA User Data located in China, as a result of the Remote Access Solution, when the order takes effect must cease being processed in China immediately at that point in time. This includes any ongoing temporary processing of EEA User Data on computer information systems in China.

705. In respect of the transfers to China, the initial transfer is made to Beijing Zitiao Network Technology Co., Ltd. and onward transfers are made by it to the further China Group Entities. TikTok Ireland stated that the access granted to the China Group Entities to EEA User Data is limited to remote access (as set out above, TikTok Ireland later informed the DPC that some EEA User Data was in fact stored on servers in China). TikTok Ireland also stated that the remote access is time limited and that the access is controlled by a set of internal web-based tools. The duration of specific remote access authorised was generally limited to no more than 12 months. To comply with the order, all such authorisations must be removed.

706. This order is appropriate in circumstances where TikTok Ireland has infringed Article 46 GDPR by carrying out the Data Transfers. Supervisory authorities are required to react appropriately to remedy infringements of the GDPR, in accordance with the means provided to them by Article 58(2) GDPR. This order is an appropriate measure to take in respect of any personal data already transferred to China and which is located in any form there as of the time when the order becomes effective, and in order to remedy the non-compliance set out in this Decision.

707. Considering the suspension order and the administrative fines in this Decision, the order to suspend transfers only concerns future data transfers and, therefore, it does not affect the personal data of EEA Users that has already been transferred by means of the Remote Access Solution when the order becomes effective and is being processed in China. Therefore, despite this suspension, the risks identified would continue to be present for data located in any form in China at that point, even on a transitory basis. Therefore, the order to suspend is the only measure that can effectively address such risks and, together with the order to suspend the transfers, restore and maintain the level of protection for the personal data of EEA Users.

708. The principle of proportionality requires that the least onerous measure be chosen and that it does not create disproportionate disadvantages in relation to the aim pursued. Recital 129 GDPR provides that consideration should be given to ensuring that measures chosen to remedy an infringement do not create *"superfluous costs"* and *"excessive inconveniences"* for the persons concerned in light of the objective pursued. The objective of this order is to ensure that processing of EEA User Data unlawfully transferred to and located in

China at the time when the order becomes effective be compliant with the GDPR. This order is proportionate to the aims pursued and reflects the least onerous measures for achieving those aims. There is a risk to EEA User Data where this data is transferred to a third country that does not provide a level of protection that is essentially equivalent, and for which, TikTok Ireland has not verified, guaranteed and demonstrated 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. As set out below, this infringement is serious in nature. Therefore, ceasing such unlawful processing in China is proportionate to the objective of bringing the processing back into compliance.

709. Furthermore, this order is necessary in the circumstances to enforce the GDPR and to achieve the protection of the data subjects with regard to the processing of their personal data. In circumstances where 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, it is necessary to make this order in order to bring the processing back into compliance. This measure is necessary to remedy an infringement and restore the level of protection of the GDPR.

O. Timeline for compliance with the suspension made pursuant to Article 58(2)(j) GDPR and the order made pursuant to Article 58(2)(d) GDPR

710. The order to suspend the Data Transfers pursuant to Article 58(2)(j) will take effect on a date 6 months from the later of (i) the date on which the period allowed for an appeal against the DPC's final decision under Section 150 of the 2018 Act has expired; and (ii) the date on which the period allowed for the bringing of an application for annulment of any decision of the EDPB under Article 263 TFEU has expired.

711. The order to bring processing into compliance pursuant to Article 58(2)(d) will take effect on a date 6 months from the later of (i) the date on which the period allowed for an appeal against the DPC's final decision under Section 150 of the 2018 Act has expired; and (ii) the date on which the period allowed for the bringing of an application for annulment of any decision of the EDPB under Article 263 TFEU has expired.

712. The DPC considers that this period for compliance with the orders is an appropriate period for TikTok Ireland, as the data exporter in respect of the Data Transfers, to ensure compliance and is a reasonable period to provide it to put an end to the transfers in the circumstances. The DPC has had regard to Project Clover and the relevant changes to the transfers that were proposed, as set out above. The DPC has also had regard to TikTok Ireland's submissions stating that this compliance period is too short given the number of TikTok users, including businesses and creators who are dependent on TikTok for their revenue, who would have to be given adequate notice and an opportunity to take mitigating steps. However, the DPC has also had regard to the risks caused to data subjects by TikTok Ireland's transfers in circumstances where the data is transferred to a third country that does not provide a level of protection that is essentially equivalent, and for which, TikTok Ireland has not verified, guaranteed and demonstrated 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. In the circumstances, the DPC finds that this period for compliance is appropriate.

713. During the said period of 6 months, TikTok Ireland will be invited to make submissions to the DPC outlining, with precision:

(i) how it will implement the suspension in a manner consistent with its obligations to Users, to include its obligations under and by reference to Chapter III of the GDPR;

(ii) how it will bring its processing into compliance in a manner consistent with its obligations to Users, to include its obligations under and by reference to Chapter III of the GDPR; and

(iii) how, and when, it will communicate its plans to Users.

714. Such submissions shall be made to the DPC not later than 2 months after the date of commencement of the above-referenced period of 6 months.

715. On receipt of such submissions, the DPC will engage with TikTok Ireland and will endeavour to agree the terms of its implementation plan within a further period of 2 months, commencing on the date of receipt of TikTok Ireland's submissions.

716. Upon receipt of such implementation plan, TikTok Ireland will be afforded a further and final period of 2 months to give effect to same such that, no later than 6 months from the date referred to above, the Data Transfers shall be suspended and TikTok Ireland's processing shall be brought into compliance.

717. For the avoidance of doubt, if TikTok Ireland fails to submit an implementation plan to the DPC within the time period noted (or at all) and/or the terms of an implementation plan cannot be agreed between the parties (whether within the time period noted, or at all), TikTok Ireland will nonetheless be bound to give effect to the order directing the suspension of the Data Transfers and the order to bring its processing into compliance no later than 6 months from the date referred to above.

P. Administrative Fines pursuant to Article 58(2)(i) GDPR

718. Article 58(2)(i) GDPR provides that a supervisory authority shall have the power:

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

719. This makes clear that the DPC may impose administrative fines in addition to, or instead of, the orders in this Decision. Section 115 of the 2018 Act mirrors this by providing that the DPC may do either or both of imposing an administrative fine and exercising any other corrective power specified in Article 58(2).

720. Article 83(1) GDPR provides:

> 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.

721. Article 83(2) GDPR provides that 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.

722. The decision as to whether to impose an administrative fine in respect of an infringement is a cumulative decision which is taken having had regard to all of the factors as set out in Article 83(2)(a) to (k). Therefore, this Decision will now proceed to consider each of these factors in turn in respect of each of the individual infringements identified in this Decision respectively.

723. For the purpose of the following assessment, *"the processing concerned"* should be understood as meaning the transfer of personal data by means of the Remote Access Solution under the controllership of TikTok Ireland to the China Group Entities. For ease of reference, the term *"the infringements"* is used throughout the following assessment to denote the infringements of Article 46(1) and Article 13(1)(f) GDPR.

a) Article 83(2)(a): the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

724. In considering the nature, gravity and duration of TikTok Ireland's infringements, the DPC has had regard to the analysis in this Decision concerning the nature, scope and purposes of the processing. Article 83(2)(a) requires that the DPC take these matters into account in having regard to the nature, gravity and duration of the infringements. Article 83(2)(a) also requires the DPC to take into account the number of data subjects affected by the infringements and the level of damage suffered by them. Therefore, this Decision will first consider these issues before proceeding to consider the nature, gravity and duration of the infringements.

725. Regarding the nature, scope and purposes of the processing concerned regarding the infringements of Articles 46(1) and Article 13(1)(f), this processing concerns TikTok Ireland's transfers of EEA User Data to China by means of remote access by the China Group Entities. The DPC has considered how these transfers concerned remote access that does not result in the bulk storage of the personal data on servers in China. The DPC has also had regard to the technical and organisational measures implemented by TikTok Ireland, as set out in this Decision. Notwithstanding, the scope of the processing was broad in circumstances where TikTok Ireland transferred the personal data for purposes that included content delivery, security, research and development, analytics, online payments, customer and technical support, and content moderation. The nature of this processing was equally broad and, as set out in the European Data Transfer Matrix, it concerned diverse matters relating to monitoring content trends, testing, and protecting the platform from fraudulent payments. As set out in the Data Transfer Assessments, this resulted in broad range of categories of personal data being transferred to China by means of remote access. Therefore, it is clear that the nature, scope and purposes of this processing resulted in systematic, repetitive, and continuous transfers of personal data to China.

726. Regarding the number of data subjects affected by the infringements, TikTok Ireland informed the DPC that in May 2022, the TikTok platform had approximately [redacted] in the EEA. TikTok Ireland has also confirmed, pursuant to its obligation under Article 24(2) of the Digital Services Act, that it had on average 125 million monthly active recipients in the European Union member state countries between August 2022 and January 2023. TikTok Ireland transferred EEA User Data for a broad variety of purposes as set out above and therefore this led to the possibility that any of these users' personal data could be transferred to China in respect of those purposes. Furthermore, each of these users were entitled to be informed of the information required by Article 13(1)(f). The personal data of any of these users of the TikTok platform in the EEA were potentially affected by the unlawful transfers and the lack of transparency because their personal data could have been subject to the transfers. Therefore, a very high number of data subjects were affected by the infringements of Articles 46(1) and 13(1)(f) GDPR.

727. In assessing the level of damage suffered by the data subjects, the DPC has had regard to the loss of control suffered by them as a result of the infringements. By transferring users' personal data to China in violation of

Article 46(1) GDPR, TikTok Ireland denied users control over their personal data by transferring their personal data to a third country that does not provide a level of protection that is essentially equivalent to EU law, and for which, TikTok Ireland has not verified, guaranteed and demonstrated 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. This also risked interferences with the fundamental rights and freedoms of data subjects.

728. Regarding transparency, Article 13(1)(f) GDPR empowers data subjects to make informed decisions about engaging with activities that cause their personal data to be processed in third countries. A lack of transparency leads to a loss of control over personal data, which, in turn, results in damage to data subjects by restricting their ability to make decisions connected to the processing of their personal data, including whether to use specific platforms. The DPC has had regard to the fact that TikTok Ireland's Privacy Policy did inform EEA Users that their personal data was transferred to third countries in general terms. However, this was not sufficient to enable data subjects to make informed decisions and exercise control over their data. To facilitate data subjects in exercising control, including by making decisions on whether to engage with the TikTok platform, those data subjects ought to have been informed that their personal data could be transferred to China specifically, and that this transfer would occur by means of remote access to personal data stored in Singapore and the United States by personnel based in China. Therefore, TikTok Ireland's infringement of Article 13(1)(f) prevented users from exercising control over their personal data.

729. TikTok Ireland does not accept that the loss of control and risk of interference with fundamental rights and freedoms regarding the infringements of Articles 46(1) and 13(1)(f) constitutes *"damage"* for the purposes of Article 83(2)(a) GDPR. In the particular circumstances of the infringements, the DPC finds that this loss of control did in fact cause damage to data subjects. Recital 75 describes the *"damage"* that can result where processing does not accord with the requirements of the GDPR:

> The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: … where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data …

730. The DPC finds that the loss of control suffered by data subjects as a result of the infringements of Articles 46(1) and 13(1)(f) GDPR caused damage to the data subjects because it restricted their ability to make informed decisions on whether to use the TikTok platform, and because the Data Transfers risked subjecting their personal data to interferences with the fundamental rights and freedoms of data subjects in circumstances where TikTok Ireland failed to verify and guarantee that the personal data would be subject to a level of protection essentially equivalent to that provided in the EEA.

731. Turning next to the nature and gravity of the infringements, the DPC considers that the nature of the infringement of Article 46(1) is serious. Articles 83(4) and (5) GDPR are directed to the maximum fine that may be imposed in respect of a particular infringement. The maximum fine prescribed by Article 83(5) GDPR is twice that prescribed by Article 83(4) GDPR. The infringements covered by Article 83(5) GDPR include infringements of Article 46(1) GDPR and Article 13(1)(f). It is therefore clear that the legislator considered these issues to be particularly significant in the context of the data protection framework as a whole. This is one factor to consider when assessing the nature of the infringements. The infringement of Article 46(1) GDPR concerns transfers of personal data to China, a third country that does not provide a level of protection that is essentially equivalent, and for which, TikTok Ireland has not verified, guaranteed and demonstrated 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. The nature of this infringement is serious in light of how the infringement related to processing that is broad in scope and in

nature, and how that infringement resulted in the data being transferred to China. The transfers are not occasional or sporadic but systematic, repetitive, and continuous in nature.

732. The gravity of the infringement of Article 46(1) is high. In assessing the gravity of the infringements, the DPC has had regard to the number of data subjects affected and the level of damage suffered by them. As set out above, a very high number of data subjects were affected by this infringement, and the DPC considers that the data subjects who were subject to the transfers suffered significant loss of control over their data. This infringement also increased the risks posed by TikTok Ireland's processing to the rights and freedoms of the data subjects.

733. The nature of the infringement of Article 13(1)(f) is also serious in nature. This infringement concerns data subjects' right to information about the transfers. Article 13(1)(f) provides that controllers must provide data subjects with information on the fact that the controller intends to transfer personal data to a third country and the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. A failure to provide this information denies data subjects an understanding of how their personal data is processed. It follows that this infringement concerns data subjects' right to information. This is a cornerstone of the rights of the data subject. The DPC has had regard to the information that was provided to data subjects, including the general reference to how personal data was transferred to third countries, however, the DPC considers that this infringement denied data subjects an understanding that their data could be subject to the transfers and the risks associated with it. Accordingly, this lack of transparency likely affected data subjects' decisions on whether to use TikTok Ireland's service and it also likely affected their decisions how they interacted with the service. The DPC does not accept TikTok Ireland's submission that the obligation on it to expressly reference China in its Privacy Policy, and to reference how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China, could not have been reasonably anticipated by it at the time. This information was crucial to data subjects' understanding of TikTok Ireland's transfers of personal data and it ought to have been clear to TikTok Ireland at the time that this information should be provided. The DPC finds that the nature of this infringement of Article 13(1)(f) is serious in nature.

734. The gravity of the infringement of Article 13(1)(f) is also high. The DPC has had regard to the very high number of data subjects affected and the level of damage suffered by them. The lack of transparency prevented those data subjects from exercising control over their personal data and increased the risks posed by the transfers as data subjects who were unaware of the transfers to China, and were denied the opportunity to take the transfers into account when deciding their use of the platform.

735. Regarding the duration of the infringement of Article 46(1), this infringement was ongoing for the entirety of the temporal scope. The DPC considers that this duration of a number of years aggravates the infringement. This duration of infringement is significant and must be taken into account when deciding whether an administrative fine should be imposed.

736. The duration of the infringement of Article 13(1)(f) began at 29 July 2020 and concluded in December 2022, when TikTok Ireland updated its Privacy Policy. Therefore, the duration of the infringement is over 2 years in length. This duration aggravates the infringement and must be taken into account when deciding whether an administrative fine should be imposed.

737. Therefore, the DPC considers that the nature, gravity and duration of the infringements are aggravating factors and the DPC has attached significant weight to these issues as aggravating factors.

b) Article 83(2)(b): the intentional or negligent character of the infringement

738. In assessing the character of the infringements, the GDPR does not identify the factors that need to be present in order for an infringement to be classified as either 'intentional' or 'negligent'. The WP29 considered this in

its 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' (the '**Administrative Fines Guidelines**') as follows:

> In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.[281]

739. The Guidelines proceed to detail how supervisory authorities should determine whether wilfulness or negligence was present in a particular case:

> The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.[282]

740. An infringement of the GDPR may be classified as intentional, negligent, or neither intentional nor negligent. In determining whether an infringement was intentional, the DPC must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration.

741. In determining whether an infringement was negligent, the DPC must determine whether, despite there being no knowledge and wilfulness in respect of the characteristics of the infringement, the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

742. TikTok Ireland's infringement of Article 46(1) GDPR concerns its transfers of personal data to China and its failure 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. Hence, the characteristics of this infringement concern those transfers of personal data and the failures to verify, guarantee and demonstrate. In order to classify this infringement as intentional, the DPC must be satisfied that (i) TikTok Ireland wilfully transferred the personal data and (ii) that it knew at the time it had not verified, guaranteed and demonstrated that that that the personal data of EEA Users is afforded a level of protection essentially equivalent to that guaranteed within the EU. While it is clear that TikTok Ireland wilfully transferred personal data to China, the DPC does not consider that the objective elements of conduct demonstrate that TikTok Ireland knew that that it had 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.

743. However, TikTok Ireland was negligent in respect of the infringement of Article 46(1) GDPR. By undertaking the Data Transfers without first verifying, guaranteeing and demonstrating 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, TikTok Ireland neglected its duty of care to data subjects. TikTok Ireland ought to have been aware of its obligations in this respect, in particular in light of the requirement for controllers and processors to verify, on a case-by-case basis whether the law of the third

[281] Article 29 Data Protection Working Party, 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of Regulation 2016/679' WP 253 (3 October 2017), at page 11.
[282] Article 29 Data Protection Working Party, 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of Regulation 2016/679' WP 253 (3 October 2017), at page 12.

country of destination ensures adequate protection, and to suspend or end the transfers if such adequate protection is not provided. TikTok Ireland breached its duty of care to a high degree of negligence.

744. TikTok Ireland submitted that its data transfer assessments and its consideration of whether EEA User Data was afforded an essentially equivalent level of protection, including the steps it undertook to assess Chinese law and practices, indicate that the infringement of Article 46(1) GDPR should not be characterised as negligent. The DPC acknowledges that TikTok Ireland carried out these assessments at the time of the Data Transfers. However, despite carrying out the assessments, TikTok Ireland was negligent to a high degree in its failure, by means of these assessments, to verify, guarantee and demonstrate that the supplementary measures and the SCCs were effective to ensure that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within the EU. Therefore, the fact that TikTok Ireland carried out these assessments does not negate the presence of negligence. TikTok Ireland ought to have been aware of the flaws in its assessments and was negligent to a high degree by carrying out the transfers despite those flaws.

745. TikTok Ireland's infringement of Article 13(1)(f) concerns its failure to provide the required information regarding the transfers to data subjects. Hence, the characteristics of this infringement concern that lack of information provided. In order to classify this infringement as intentional, the DPC must be satisfied that (i) TikTok Ireland wilfully omitted to provide the information and (ii) that it knew at the time that it did not provide the information required. In making this determination, the DPC must rely on objective elements of TikTok Ireland's conduct that show the presence or absence of wilfulness and knowledge. During the Inquiry, TikTok Ireland outlined the various processes that it put in place with regard to providing data subjects with relevant information on its transfers of personal data to third countries. The objective elements of TikTok Ireland's conduct do not suggest that it knew, during the temporal scope, that this information ought to have expressly referenced China and how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China. The DPC accepts that the objective elements of conduct during the temporal scope of the Inquiry suggest that TikTok Ireland believed that it had provided the required information to data subjects, and that it had done so in a manner that complied with its obligations.

746. However, TikTok Ireland's infringement of Article 13(1)(f) was negligent in the particular circumstances. TikTok Ireland ought to have been aware of how its transparency obligations in the circumstances necessitated information to be provided in a manner that informed data subjects of the transfers to China and how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China.

747. TikTok Ireland submitted that it could not reasonably have anticipated these requirements by reference to Article 13(1)(f) in circumstances where there was no guidance or published decision of the DPC or the EDPB interpreting Article 13(1)(f) as requiring same at the time. The DPC has had particular regard to how a company the size of TikTok Ireland ought to have been aware of its precise transparency obligations and how the nature of TikTok Ireland's business entails processing large volumes of personal data. In those circumstances, irrespective of the level of guidance available at the time relevant to compliance with Article 13(1)(f), the DPC finds that TikTok Ireland ought to have been aware of the extent of its obligations under Article 13(1)(f). Therefore, the DPC finds that TikTok Ireland was negligent within the meaning of Article 83(2)(b).

748. TikTok Ireland submitted that a finding that an infringement was negligent, rather than intentional, ought to be treated as mitigating. The DPC finds that the degree of negligence present in each of the infringements of Articles 46(1) and 13(1)(f) respectively mean that the negligence regarding these infringements must be treated as aggravating in the circumstances. Therefore, the DPC finds that the negligent nature of the infringements is an aggravating factor of significant weight.

c) Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects

749. The DPC notes that TikTok Ireland considered that the processing concerned was being carried out with a valid lawful basis at the relevant times and throughout the course of the inquiry. Therefore, the DPC does not consider that TikTok Ireland could have been expected to take action *"to mitigate the damage suffered by data subjects"* in circumstances where it did not consider any infringement to have occurred or any damage to have been suffered by data subjects. In the circumstances, the DPC considers that nothing arises for consideration under this heading and that this factor is neither aggravating nor mitigating in the circumstances.

750. TikTok Ireland disagrees with this assessment and submitted that TikTok Ireland's transition to the 2021 SCCs and its updates to its supplementary measures throughout the Inquiry have acted to mitigate any possible adverse effects or damage to data subjects. The DPC does not accept that TikTok Ireland has mitigated the damage suffered. As set out above, by transferring users' personal data to China in violation of Article 46(1) GDPR, TikTok Ireland denied users control over their data by transferring their personal data to a third country that does not provide a level of protection that is essentially equivalent to EU law, and for which, TikTok Ireland has not verified, guaranteed and demonstrated 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. This also risked interferences with the fundamental rights and freedoms of data subjects. TikTok Ireland's transition to the 2021 SCCs and its updates to its supplementary measures do not act to mitigate the loss of control suffered by data subjects as a result of the infringements identified in this Decision. Therefore, the DPC finds that this factor is neither aggravating nor mitigating in the circumstances.

751. The DPC notes the changes made by TikTok Ireland to its transparency information in December 2022. However, the DPC considers that this factor is relevant to the duration of the infringement, and does not constitute action taken to mitigate damage suffered. The DPC does not accept TikTok Ireland's submission that the update to its Privacy Policy mitigated the damage to data subjects as a result of the infringement of Article 13(1)(f). The subsequent provision of this information cannot act to mitigate the loss of control suffered by data subjects in respect of decisions connected to the processing of their personal data, including whether to engage with the TikTok platform, before this information was provided to data subjects. Data subjects who became aware of this information as a result of the update to the Privacy Policy risked already having had their personal data transferred to China as a result of their use of the TikTok platform, and their subsequent awareness of this possibility cannot act to mitigate the loss of control already suffered and the restriction on their ability to make decisions connected to the processing of their personal data.

752. The DPC does not accept TikTok Ireland's submission[283] that its updated Privacy Policy provided data subjects with information that went beyond what TikTok Ireland was obliged to provide to data subjects pursuant to its obligation under Article 13(1)(f) GDPR. The DPC accepts that the updated Privacy Policy was sufficient to comply with Article 13(1)(f) in the context of the Data Transfers subject to the material scope of this Decision, but does not accept TikTok Ireland's position that it provided additional information beyond that which was required by Article 13(1)(f) GDPR.

753. Therefore nothing arises for consideration under this heading and that this factor is neither aggravating nor mitigating in the circumstances.

[283] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at paragraph 512.

d) Article 83(2)(d): the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

754. The Article 29 Working Party Administrative Fines Guidelines set out that:

> The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.[284]

755. The DPC considers that TikTok Ireland holds a high degree of responsibility for the infringements identified in this Decision taking into account the technical and organisational measures implemented pursuant to Article 25 GDPR.

756. Article 25(1) GDPR states:

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

757. The DPC has set out above that TikTok Ireland did not do what it could be expected to do in respect of verifying, guarantying and demonstrating 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, and in providing information to data subjects on the transfers. The duty rests with TikTok Ireland to identify and implement such appropriate measures and for the reasons set out in this Decision, TikTok Ireland has failed to do so. TikTok Ireland holds a high degree of responsibility in light of the absence of appropriate technical and organisational measures implemented in pursuit of these objectives. Given the nature, purposes and size of TikTok Ireland's processing, it ought to have implemented measures to ensure these matters and it holds a high degree of responsibility for its failure to do so. Therefore, the DPC considers that this factor is an aggravating factor of significant weight in respect of both infringements.

e) Article 83(2)(e): any relevant previous infringements by the controller or processor

758. No relevant previous infringements arise for consideration in this context. This factor is neither aggravating nor mitigating in the circumstances.

f) Article 83(2)(f): the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

759. TikTok Ireland cooperated fully with the DPC at all stages of the Inquiry, as it is required to do so by law. In the circumstances, nothing arises for assessment by reference to this criterion and the DPC considers that this factor is neither aggravating nor mitigating in respect of the infringements.

---

[284] Article 29 Data Protection Working Party 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of Regulation 2016/679' WP 253 (3 October 2017), at page 13.

760. TikTok Ireland submitted that its issuing of the Updated Privacy Policy and the new measures that it has implemented since the Inquiry commenced ought to be treated as a mitigating factor under Article 83(2)(f). The DPC has already considered, within the Article 83(2)(c) assessment, above, the actions taken by TikTok Ireland in an effort to mitigate the possible adverse effects of the Infringement on data subjects. While TikTok Ireland took action to address its ongoing non-compliance regarding Article 13(1)(f) GDPR during the Inquiry, this issue relates to the duration of that infringement, and the DPC does not consider that the action relied upon by TikTok Ireland has mitigated the possible effects of the established infringements. Therefore, this factor is neither aggravating nor mitigating in respect of the infringements.

g) Article 83(2)(g): the categories of personal data affected by the infringement

761. TikTok Ireland's Data Transfer Assessments contained an outline of the categories of the personal data of EEA Users of the TikTok platform the subject of the Data Transfers during the temporal scope of the Inquiry. As set out above, these categories included, amongst others, various identifiers; user generated content including video content, audio files, comments and direct message content; Ads data, including ad campaign conversion; location; payment information, including bank account details; survey responses; and other categories.

762. Therefore, TikTok Ireland transferred a large number of broad categories of personal data to China and a large number of categories of personal data have been affected by the infringements. Much of the categories of data transferred to China represent categories that deserve a stricter response in terms of the decision on whether to impose fines and, if so, the quantum of the fines. These categories included data the dissemination of which is likely to cause immediate damages or distress to the data subjects, such as data about users' daily lives and interests, location data, data on private communication, and financial data, all of which are included in the categories transferred by TikTok Ireland to China.

763. Furthermore, the personal data transferred included data that is capable of revealing special category data pursuant to Article 9 GDPR. TikTok Ireland stated that, while the processing undertaken by the China Group Entities is not for the purpose of revealing or deducing special category data, personal data which could potentially be capable of revealing special category data may be processed incidentally by TikTok or uploaded by EEA Users on the Platform. In light of the categories of personal data transferred to the China Group Entities, including user generated content and direct message content, the DPC considers this personal data included data that is capable of revealing special category data.

764. In light of the categories of personal data affected by the infringements, this factor must be taken into account as an aggravating factor when deciding on whether a fine should be imposed. The DPC attached significant weight to this factor as an aggravating factor.

h) Article 83(2)(h): the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

765. The infringements became known to the DPC as a result of this own volition inquiry. In those circumstances, the DPC finds that this factor is neither aggravating nor mitigating.

i) Article 83(2)(i): where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

766. Corrective powers have not previously been ordered against TikTok Ireland with regard to the subject matter of this Decision. The DPC finds that his factor is neither aggravating nor mitigating.

j) Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

767. The DPC finds that nothing arises for assessment under this heading.

k) Article 83(2)(k): any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

768. TikTok Ireland referred to the harm that it contends would be caused to its business as a result of the Suspension Order as a mitigating factor. The DPC accepts that the orders in this Decision will have adverse financial consequences for TikTok Ireland. The DPC has had regard to such consequences and finds that this is a mitigating factor of moderate weight. Therefore, the fines specified in this Decision take appropriate account of the fact that they will be imposed on TikTok Ireland in addition to the orders specified above. The DPC finds that there are no further aggravating or mitigating factors present in respect of the infringements.

769. Having regard to the requirement to ensure the fines imposed are effective, proportionate and dissuasive in accordance with Article 83(1) GDPR, the DPC considers it necessary to have regard to the turnover of ByteDance Ltd, as detailed below, when assessing the quantum of the fines. The DPC's assessment of the undertaking concerned and the applicable turnover figure is detailed further below. While this is not a matter that can properly be classified as either mitigating or aggravating, by reference to the circumstances of the case, the DPC has taken the significant turnover of the undertaking concerned into account when determining the quantum of the fines, as set out below.

i. Decision on whether to impose administrative fines

770. In deciding whether to impose an administrative fine in respect of each infringement, the DPC has had regard to the factors outlined in Article 83(2)(a) – (k) cumulatively, as set out above. However, the DPC has considered each of the infringements separately when applying those factors, when deciding whether to impose an administrative fine, and when deciding the amount of each administrative fine. The DPC has also had regard to the effect of the orders in ensuring compliance with the GDPR. The orders will assist in ensuring compliance by mandating specific action on the part of TikTok Ireland in order to re-establish compliance with specific findings of infringements. However, these measures alone are not sufficient in the circumstances to ensure compliance. The DPC finds that administrative fines in respect of each of the infringements are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

771. In order to ensure compliance with the GDPR, it is necessary to dissuade non-compliance. Depending on the circumstances of each individual case, dissuading non-compliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. Where a serious infringement of the GDPR occurs, orders alone may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 of the GDPR acknowledges that, depending on the

circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, orders and other corrective powers:

> In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.

772. While the orders in this Decision will re-establish compliance with the specific infringements identified, the DPC does not consider these measures sufficient to deter other future serious infringements. The DPC finds that administrative fines are necessary in respect of each of the infringements to deter other future serious non-compliance on the part of TikTok Ireland and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

(i) In coming to the conclusion that administrative fines are necessary, the DPC has had particular regard to the nature, gravity and duration of the infringements. The DPC has attached significant weight to these issues as aggravating factors. The duration of the infringements were lengthy and administrative fines are proportionate in terms of such infringements. In circumstances where a large number of data subjects were affected by the transfers and the lack of transparency, where the scope of the relevant processing was broad, and whereby those data subjects suffered a loss of control over their personal data, it is necessary, appropriate and proportionate to impose administrative fines in order to deter non-compliance.

(ii) The DPC also attaches significant weight, as an aggravating factor, to the negligent nature of the infringements, because a sophisticated entity such as TikTok Ireland, ought to have known that its provision of information to data subjects fell short of the standards required, and the extent of its obligation 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, or in the alternative to end or suspend the transfers.

(iii) The DPC also attaches significant weight as an aggravating factor to TikTok Ireland's high degree of responsibility in light of the absence of appropriate technical and organisational measures implemented in pursuit of verifying, guaranteeing and demonstrating that the supplementary measures and the SCCs are effective in ensuring that the personal data of EEA users is afforded a level of protection essentially equivalent to that guaranteed within the EU and in transparently providing the information required under Article 13(1)(f) GPPR. The absence of such measures is stark in light of the scope of the relevant processing.

(iv) The DPC also attaches significant weight to the categories of personal data affected by the infringements. In light of the broad categories of personal data affected, and the sensitive nature of some of that data, administrative fines are necessary to deter non-compliance in respect of this type of data.

773. For the reasons set out above, and having particular regard to the matters discussed under Article 83(2)(a)-(k) cumulatively, the DPC considers it appropriate to impose administrative fines in respect of both of the infringements, in addition to the orders also imposed in this Decision. Based on the analysis set out in this Decision, and following its consideration of the views of the two CSAs who made comments on the administrative fines proposed in the Draft Decision, and the subsequent further submissions of TikTok Ireland on those views and on the question of the appropriate fines, the DPC has decided to impose the following administrative fines in respect of TikTok Ireland's infringements:

(i) TikTok Ireland's infringement of Article 46(1): a fine of €485 million; and

(ii) TikTok Ireland's infringement of Article 13(1)(f): a fine of €45 million.

774. The total of these fines is €530 million.

775. In having determined the quantum of the fines above, the DPC has taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be *"effective, proportionate and dissuasive"* in each individual case. In order for any fine to be effective, it must reflect the circumstances of the individual case. As outlined above, the infringements are all serious in nature and high in gravity. The infringements concern transfers of personal data to China in circumstances where TikTok Ireland 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.

776. In order for a fine to be dissuasive it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. The DPC considers that the fines are dissuasive for both.

777. As regards the requirement for any fine to be proportionate, this requires the DPC to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. Proportionality is a principle of EU law that requires a measure to pursue a legitimate objective, be appropriate to attain that objective, and not go beyond what is necessary to achieve the objective.

778. TikTok Ireland has submitted that administrative fines in the ranges proposed in the Preliminary Draft Decision and the Draft Decision were not necessary nor appropriate to deter non-compliance and that the suspension order alone would act as a sufficient deterrent. TikTok Ireland also referred to its Updated Privacy Policy and Project Clover in arguing that administrative fines in the ranges proposed are not necessary to deter non-compliance.

779. The DPC does not accept TikTok Ireland's submissions in this regard. The objectives of the administrative fines in this case are to both re-establish compliance with the rules, and to sanction TikTok Ireland's infringements. As regards the requirement for any fine to be necessary in respect of these objectives, this requires the DPC to adjust the quantum of any proposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. The DPC is satisfied that the fines imposed, which are within the ranges proposed in the Preliminary Draft Decision and the Draft Decision, do not exceed what is necessary to enforce compliance with the GDPR taking into account the number of data subjects affected, the unlawfulness of the transfers and the lack of transparency, the loss of control over personal data suffered by the data subjects, and the scope of the processing and categories of personal data affected by the infringements. The DPC has also had regard to the turnover of ByteDance Ltd, as detailed below. The DPC is satisfied that the fines imposed on TikTok Ireland are effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry. The DPC is satisfied that these fines do not exceed the minimum necessary to enforce compliance with the GDPR provisions found to have been infringed.

780. TikTok Ireland submitted that the fines proposed in the Preliminary Draft Decision and the Draft Decision were disproportionate in circumstances where, according to TikTok Ireland, *"the DPC's finding is one of demonstration rather than substance."*[285] For the reasons set out in this Decision, the finding of infringement regarding Article 46 GDPR must be characterised as one of substance. The obligation on controllers or processors to verify and guarantee that transfers made under Article 46 GDPR are subject to a level of

[285] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at page 142.

protection essentially equivalent to that which is guaranteed in the European Union is crucial to upholding the fundamental rights of data subjects. This responsibility applies in the context of the risk that the protection afforded within the European Union can be undermined when personal data moves across borders outside the European Union. It is essential that the controller or processor first verify and guarantee an essentially equivalent level of protection. This is how Article 46 GDPR ensures that the high level of that protection provided within the European Union continues where personal data is transferred to a third country. In order for TikTok Ireland to rely on Article 46 for the Data Transfers, TikTok Ireland was obliged to first verify and guarantee an essentially equivalent level of protection. A failure on TikTok Ireland's part to do so mandates that TikTok Ireland, or failing that, the DPC, suspend or end the transfers. The Schrems II judgment is clear that where a controller or processor cannot guarantee the essentially equivalent protection, that controller or processor is required to suspend or end the transfer. This is at the core of upholding the fundamental rights of data subjects and upholding the level of protection afforded by, inter alia, the GDPR. Therefore, TikTok Ireland's infringement of Article 46 is a very substantial infringement.

ii. Article 83(3) GDPR

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

782. Article 83(3) GDPR provides that:

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

783. TikTok Ireland submitted that the meaning of Article 83(3) GDPR is that *"if there are several infringements for the same or linked processing operations, then the total fine imposed shall not exceed the amount of the fine specified for the gravest infringement."* The DPC does not accept TikTok Ireland's submissions in that regard, having particular regard to the EDPB's adoption of a binding decision relating to IN 18-12-2[286], an inquiry conducted by the DPC into WhatsApp Ireland Limited's compliance with transparency obligations under the GDPR. Rather, consistent with that binding decision, in the case of multiple infringements arising from *"the same or linked processing operations"*, Article 83(3) acts to limit the amount of the administrative fines imposed to the amount specified for the gravest infringement. This refers to the legal maximum of fines under Articles 83(4), (5) and (6) GDPR. This requires that other infringements have to be taken into account when assessing the amount of the fine. However, the fine imposed must not exceed the legal maximum of the highest fining tier and the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR. However, the other infringements cannot be discarded but have to be taken into account when calculating the fine.

784. The relevant passage of the EDPB decision is as follows:

> All CSAs argued in their respective objections that not taking into account infringements other than the "gravest infringement" is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be

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

for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.

The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.

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

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

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

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

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

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

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

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

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

Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.

In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness.[287]

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

786. TikTok Ireland's infringement of Article 46(1) is the gravest infringement. This is for the reasons as set out above. The DPC notes that the associated maximum possible fine for that infringement under Article 83(5)

[287] Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021, at paragraphs 315 – 326.

GDPR is 4% of the turnover of ByteDance Ltd. It is further to be noted that the EDPB Decision quoted above also directed the DPC to take account of the undertaking's turnover in the calculation of the fine amounts and the DPC has factored that turnover figure into the calculations of the individual fines. When the fines for the individual infringements are added together, a total fine of €530 million arises. The combined fines are below 4% of the turnover of ByteDance Ltd. as considered below.

787. TikTok Ireland also submitted that the imposition of two separate fines in this Inquiry would amount to *"[imposing] multiple penalties for a single course of conduct".*[288] As set out above, the fine for the infringement of Article 46(1) GPDR is imposed in respect of TikTok Ireland's carrying out the Data Transfers while failing to verify, guarantee and demonstrate that 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. On the other hand, the fine for the infringement of Article 13(1)(f) GPDR is imposed in respect of TikTok Ireland's failure to provide data subjects with information on its transfers of personal data to China and information on how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China. Therefore, the DPC finds that these infringements are applicable alongside each other in terms of the administrative fines imposed.

iii. Article 83(5) GDPR

788. Turning, finally, to Articles 83(5) GDPR, this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

789. Article 83(5) provides as follows:

> Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
>
> […]
>
> (b) the data subjects' rights pursuant to Articles 12 to 22;
>
> (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
>
> […]

790. In order to determine the applicable fining cap, it is firstly necessary to consider whether or not the fine is to be imposed on *"an undertaking"*. Recital 150 clarifies, in this regard, that:

[288] TikTok Ireland's submissions, dated 9 September 2023, in response to the Preliminary Draft Decision, at page 142 at page 146.

> Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.

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

> an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed[289]

792. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement.[290]

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

794. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case.[291]

795. The CJEU has, however, established that, where a parent company has a 100% shareholding in a subsidiary, it follows that the parent company is able to exercise decisive influence over the conduct of the subsidiary; and a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.[292]

796. The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is

---

[289] Case C-41/90, Höfner and Elser v Macrotron GmbH, judgment of 23 April 1991 (ECLI: EU:C:1991:161), at paragraph 21.
[290] Case C-97/08 P, Akzo Nobel and Others v Commission, judgment of 10 September 2009 (ECLI:EU:C:2009:536) at paragraphs 58-60.
[291]Case C-490/15 P, Ori Martin and SLM v Commission, judgment of 14 September 2016 (ECLI:EU:C:2016:6780 at paragraph 60.
[292] Case C-97/08 P, Akzo Nobel and Others v Commission, judgment of 10 September 2009 (ECLI:EU:C:2009:536).

also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary.[293]

797. The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise decisive influence over the conduct of its subsidiary.[294] This reflects the position that:

> … the presumption of actual exercise of decisive influence is based, in essence, on the premise that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day business of that subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company…[295]

798. Where the presumption of decisive influence has been raised, it may be rebutted by the production of sufficient evidence that shows, by reference to the economic, organisational and legal links between the two entities, that the subsidiary acts independently on the market.

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

800. Per TikTok Ireland's Director's Report and Financial Statement for year ending 31 December 2021, available from the Companies Registration office, TikTok Ireland is a private company limited by shares, incorporated on 12 October 2018. TikTok Ireland's sole shareholder is TikTok Information Technologies UK Limited. TikTok Ireland confirms therein that its ultimate parent is ByteDance Ltd.

> TikTok Technology Limited is a private company limited by shares (registered under Part 2 of Companies Act 2014), incorporated in the Republic of Ireland, under the registered number 635755. The registered office and place of business is 10 Earlsfort Terrace, Dublin 2, D02 T380, Ireland. The

[293] Case C-508/11 P, Eni v Commission, judgment of 8 May 2013 (ECLI:EU:C:2013:289) at paragraph 48.
[294] Case T-206/06, Total and Elf Aquitaine v Commission, judgment of 7 June 2011, (ECLI:EU:T:2011:250) at paragraph 56; and Case T-562/08, Repsol Lubricantes y Especialidades and Others v Commission, judgment of 12 December 2014, (ECLI:EU:T:2014:1078) at paragraph 42; and Cases T-413/10 T-414/10, Socitrel - Sociedade Industrial de Trefilaria, SA and Companhia Previdente-Sociedade de Controle de Participações Financeiras, SA v European Commission, judgment of 15 July 2015 (ECLI:EU:T:2015:500) at paragraph 204.
[295] Case C-97/08 P, Opinion of Advocate General Kokott in Akzo Nobel and Others v Commission, opinion of 23 April 2009, (ECLI:EU:C:2009:262) at paragraph 73, as cited in Case T-419/14, Goldman Sachs Group, Inc. v European Commission, judgment of 12 July 2018 (ECLI:EU:T:2018:445) at paragraph 51.

> principal activity of the Company is that of providing services related to content moderation, data controlling of TikTok in EEA, and sales, marketing and routine support to other group companies.
>
> TikTok Information Technologies UK Limited owns 100% of the equity share capital of Tiktok Technology Limited.
>
> Tiktok Technology Limited's ultimate parent is Bytedance Ltd., a company incorporated and registered in Cayman. TikTok Information Technologies UK Limited prepares group financial statements and is the smallest group for which group financial statements are drawn up and of which Tiktok Technology Limited is a member. Copies of the TikTok Information Technologies UK Limited group financial statements are available from the Company Secretary at its registered office One London Wall 6th Floor, London, EC2Y 5EB, England.[296]

801. It seemed therefore, that the corporate structure of the entities concerned is such that ByteDance Ltd. is in a position to exercise decisive influence over TikTok Ireland's behaviour on the market. Accordingly, a rebuttable presumption arose to the effect that ByteDance Limited does in fact exercise a decisive influence over the conduct of TikTok Ireland on the market. The DPC notified TikTok Ireland of this presumption.

802. On 26 April 2023, the DPC wrote to TikTok Ireland setting out the concept of undertaking and how it applies in the context of the GDPR and detailing the DPC's understanding of the relevant factors, as they appear to apply to TikTok Ireland. On 12 May 2023, TikTok Ireland informed the Inquiry that it did not agree with the DPC's assessment. TikTok Ireland also provided the Inquiry with a corporate structure chart, which confirms that Bytedance Ltd has a 100% shareholding in TikTok Limited (Cayman), which has a 100% shareholding in TikTok Information Technologies UK Ltd, which has a 100% shareholding in TikTok Technology Limited. In TikTok Ireland's letter dated 12 May 2023, it stated that:

> ByteDance Ltd. is a Cayman Island entity which is not involved in the operation of the TikTok platform, but is instead a holding company which has ownership interests in a diverse range of businesses. TikTok is just one of the numerous business lines in which ByteDance Ltd. has ownership interests.

803. However, the DPC finds that the information submitted by TikTok Ireland is not sufficient to rebut the presumption of decisive influence. TikTok Ireland has not produced any evidence that shows, by reference to the economic, organisational and legal links between the entities, that the TikTok Ireland acts independently on the market.

804. As this presumption was not rebutted, it means that ByteDance Ltd and TikTok Ireland constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant cap for the purpose of Articles 83(4) and (5) GDPR, falls to be determined by reference to the combined turnover of TikTok Ireland and ByteDance Ltd.

805. With regard to the relevant year for the calculation of turnover, Article 83(5) states that the fining cap is *"in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year"*. The DPC disagrees with TikTok Ireland's submission that the correct year is the financial year preceding the

[296] TikTok Technology Limited, 'Director's Report and Financial Statement' (Year Ending 31 December 2021), at page 11.

date of the infringement. Rather, the DPC finds that the relevant year is the year prior to the decision to impose an administrative fine. As noted by the EDPB in Binding Decision 1/2021, in the case of cross-border processing, the relevant fining decision is not the draft decision, but rather the final decision issued by the Lead Supervisory Authority. The DPC therefore uses the best available and most up to date financial information in making this calculation.

806. On 18 April 2025, TikTok Ireland informed the DPC that the unaudited annual turnover figure for ByteDance Ltd for the year ending 31 December 2024 was [redacted][297]

807. Applying the above to Article 83(5) GDPR, in circumstances where the fine is being imposed on an undertaking, a fine of up to 4% of the total worldwide annual turnover of the preceding financial year may be imposed. In relation to the above, the DPC notes that the fines do not exceed the applicable fining 'cap' prescribed by Article 83(5) GDPR in relation to ByteDance Ltd. total annual turnover for the year 2024.

iv. Selection of Amounts of the Administrative Fines

808. TikTok Ireland's submissions in response to the CSA Comments submitted that the DPC ought to fix the administrative fines at the lower end of the fining ranges and that the Article 83(2) factors do not warrant fines at the upper end of the fining ranges. TikTok Ireland submitted that fines at the upper end of the fining ranges would not satisfy the requirement that administrative fines imposed must be effective, proportionate and dissuasive. In support of this view, TikTok Ireland repeated certain submissions that were previously made and which have already been taken into account elsewhere in this Decision. For example, TikTok Ireland repeated its earlier position that the DPC failed to have adequate regard to the actions taken by TikTok Ireland to mitigate damage to data subjects; it repeated submissions made previously regarding measures implemented by Project Clover; and it referred to the impact of the suspension order and the order to bring processing into compliance. In circumstances where the DPC has already addressed these matters in coming to this Decision, it is not necessary to repeat its position on such previously assessed matters here.

809. TikTok Ireland also submitted that the DPC is ought to treat negligence as a mitigating factor, or at the very least, as neutral under Article 83(2)(b). TikTok Ireland cites in support of this the judgment of the CJEU in NVSC[298]. TikTok Ireland cites this judgment in arguing that as negligence is a minimum precondition to the imposition of a fine, it follows that negligence cannot be *"an aggravating factor of significant weight"*.

810. The DPC does not accept this interpretation of the CJEU's judgment or TikTok Ireland's argument on how it should be applied in this case. The DPC accepts, as found in the CJEU's judgment, that *"only infringements of the provisions of that regulation which are committed wrongfully by the controller, that is to say, those committed intentionally or negligently, may result in an administrative fine being imposed on that controller pursuant to that article.*" However, the judgment does not state or infer that negligence should be considered a mitigating factor. Negligence is commonly a matter of degree, which can range from minor oversights to serious dereliction of responsibility. Fines in such cases should be set at a level that reflects the degree of negligence found. The ranges of fines proposed in the Draft Decision reflected, and were premised on, the DPC's assessment of the facts and TikTok Ireland's submissions, as set out in that document. These included the DPC's findings of negligence. If the DPC had concluded that the infringements found in this case were

[297] TikTok Ireland noted that this figure was unaudited and subject to change.
[298] Case C-683/21 *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija* EU:C:2023:949.

intentional, rather than negligent, it would most probably have proposed administrative fines considerably higher than those that it did. The DPC is accordingly of the view that it has correctly taken account of negligence in this case and is not persuaded by TikTok Ireland's submission on this issue to select a lower level of administrative fines.

811. TikTok Ireland submitted that, in terms of the risk to the rights and freedoms of data subjects, the findings in the Draft Decision were narrowed when compared with the Preliminary Draft Decision. According to TikTok Ireland, the resulting risk to data subjects is lower. The DPC does not accept TikTok Ireland's submissions in this regard and the DPC also does not accept TikTok Ireland's position that there has been a significant reduction in the likelihood and severity of the risk. TikTok Ireland's ongoing failures regarding the scope of the problematic laws, the contours of the territoriality principle, and the application of the territoriality principle in practice in a scenario concerning remote access pose very significant risks to the rights and freedoms of data subjects. These risks were considered in the Preliminary Draft Decision and the risks remain in circumstances where the transfers of EEA User Data to China are ongoing. The DPC does not accept TikTok Ireland's position that it has adequately assessed the applicability of Chinese law, including the territoriality principle, in relation to EEA User Data temporarily processed on computer information systems in China as a result of remote access to EEA User Data stored on servers outside China. Having regard to the systematic, repetitive, and continuous nature of the transfers of personal data to China, the DPC does not accept that there is a material *"reduced risk to the rights and freedoms of data subjects"*.

812. The DPC has had regard to TikTok Ireland's submissions regarding the adverse financial consequences that will be caused to TikTok Ireland's business as a result of the suspension order. As set out above, this is a mitigating factor of moderate weight and the DPC has had regard to this when selecting the fines

813. The DPC does not, however, accept TikTok Ireland's submission that [redacted] is a mitigating factor in the particular circumstances of this inquiry in terms of the quantum of the fines, and the DPC notes in this regard, the need for administrative fines to have a dissuasive effect.

814. TikTok Ireland submitted that its ability to make meaningful submissions in response to the CSA Comments was curtailed because the DPC did not provide its provisional views in relation to the determination of the specific fine amounts. TikTok Ireland submitted that the refusal by the DPC to provide its provisional views in relation to the determination of the specific fine amounts interfered with its ability to make meaningful submissions in respect of the quantum of the administrative fines, having regard in particular to the magnitude of the fines being contemplated and the breadth of the fining ranges. The DPC does not accept these submissions and considers that TikTok Ireland has had ample opportunity to make its submissions on the CSA Comments and on the selection of the amounts of the administrative fines. As set out in the DPC's correspondence to TikTok Ireland dated 11 April 2025, the DPC's final determination regarding the fines in this Decision is based on: (a) the DPC's assessment of the criteria outlined in Articles 83(1) and (2) GDPR (as already recorded in the Draft Decision); (b) the views that were expressed by the CSAs, along with; (c) TikTok Ireland's additional submissions. TikTok Ireland was provided with the Preliminary Draft Decision on 17 May 2023 and provided extensive responding submissions in respect of the application of the criteria in Articles 83(1) and (2) GDPR. The DPC took those submissions fully into account when drafting the Draft Decision. Following the Article 60 GDPR process, the DPC also provided TikTok Ireland with the CSA Comments on the Draft Decision, in full, and provided information as to how it interpreted those comments relating to the selection of the specific quantum of the administrative fines, from within the identified fining ranges, pending any submissions that TikTok Ireland wished to make in relation to them. The DPC further took into account the submissions made by TikTok Ireland on 11 April 2025. The DPC is therefore satisfied that TikTok Ireland's ability to make meaningful submissions on this aspect of matters was in no way compromised and that it was furnished with all relevant information to allow it do so.

The views expressed by the French SA and German SAs regarding the level of the fine

815. As set out above, in response to the Draft Decision circulated under Article 60(3) GDPR, the French, the Netherlands and the German SAs provided views to the DPC. The views of the French and German SAs included views on the administrative fines.

816. The cooperation mechanism outlined in Article 60 GDPR requires the lead supervisory authority (in this case, the DPC) to take due account of the views expressed by CSAs in response to a draft decision. This is clear from the text of Article 60(3) GDPR. That obligation applies regardless of whether the views have been expressed in the form of a relevant and reasoned objection or otherwise in the form of comments, as on this occasion.

817. In its response to the CSA Comments, TikTok Ireland submitted that *"While the DPC is required to take due account of the comments of the CSAs, they are not binding on the DPC."* In this regard, TikTok Ireland contrasted the requirement to take due account of views expressed by CSAs in response to the submission of a draft decision under Article 60(3) with the status of a relevant and reasoned objection made by a CSA under Article 60(4) GDPR. TikTok Ireland noted that the GDPR imposes rigorous obligations and assessment processes to ensure that objections meet the *"relevant and reasoned"* thresholds identified in Article 4(24) GDPR, which do not apply to comments. Accordingly, TikTok Ireland submitted, the DPC is not obliged to amend the Draft Decision on foot of comments expressed by CSAs. In respect of the requirement to take due account, TikTok Ireland submitted that this requires the DPC to take note of the Comments, but that the DPC cannot make any material amendments to the Draft Decision to give effect to the Comments.

818. The DPC agrees with this analysis of its obligation to take due account of CSA Comments under Article 60(3) GDPR, both in respect of comments relating to the administrative fines, and in respect of comments regarding other elements of the Draft Decision. The DPC agrees that it is not under an obligation to give effect to these comments in the Final Decision and that it cannot make a material amendment to the Draft Decision. However, for the reasons that follow, the DPC does not accept TikTok Ireland's position that the DPC should not be influenced in the particular circumstances by the views in determining the specific fine amounts.

819. In response to the Draft Decision, the German SAs made the following comment:

> …While we understand that it is not possible to include the most recent Fining Guidelines 04/2022 without triggering a new right to be heard, we would like to suggest using the turnover of the year 2024 as the basis for calculating the administrative fine. We therefore ask the DPC to consider using more recent figures in this context. The DD currently refers to the turnover of year 2023 (para 778). Article 83(5) GDPR instead provides that "infringements [...] shall, in accordance with paragraph 2, be subject to administrative fines [...] up to 4 % of the total worldwide annual turnover of the preceding financial year". If the final decision of the DPC is issued in 2025, the annual turnover of 2024 would be the appropriate basis to calculate the administrative fine…

820. As set out above, the DPC has taken account of the 2024 turnover of ByteDance ltd for the purposes of this Decision. Regarding the reference in that comment to the EDPB Fining Guidelines 04/2022, the Draft Decision did not make reference to those guidelines because the Preliminary Draft Decision (by reference to which TikTok Ireland was afforded its right to be heard) was prepared prior to the adoption, by the EDPB, of the Fining Guidelines. The DPC notes, in any event, that the criteria that must be used by supervisory authorities, in order to decide whether or not to impose an administrative fine and, if so, the amount of any such fine, are set out in Articles 83(1) and (2) GDPR. The purpose of the Fining Guidelines it to enable a harmonised approach to these assessments. The Fining Guidelines do not supplant (or purport to supplant) the primary criteria that must be used to determine fining matters, as set out in Article 83 GDPR itself. In these circumstances, the fining ranges set out in the Draft Decision took account of the criteria forming the basis of the Fining Guidelines.

821. In response to the Draft Decision, the French SA made the following comment:

> …With regard to the total amount of the proposed fine : the chair of the restricted committee agrees with the DPC's analysis about the seriousness of the breaches and insists on the fact that, given the nature of the breaches and the number of people concerned, the total amount of the fines should reach the upper range proposed, i.e. 550 million euros.

822. Accordingly, the French SA expressly states that the administrative fines should reach the upper end of the proposed fining ranges. This view refers to the seriousness of the infringements, the nature of the infringements, and the number of data subjects affected, as assessed by the DPC pursuant to Article 83(2)(a) GDPR. Therefore, the French SA has clearly identified factors in the Decision that it considers are in favour of the selection of administrative fines from the upper end of the proposed fining ranges. The DPC has taken due account of those views in exercising its discretion in the selection of the administrative fines.

823. TikTok Ireland disagreed and submitted that the DPC should not place any weight on the comment of the French SA and also submitted that the administrative fines should be fixed at the lower end of the fining ranges set out in the Draft Decision. TikTok Ireland submitted that the French SA's comment is inadequately reasoned and does not identify any basis for fixing the administrative fines at the upper end of the finings ranges.

824. In considering the views made regarding the administrative fines, and TikTok Ireland's submission on this matter, it is important to recall that the DPC's final determination of the specific fines to be imposed from within any proposed fining range does not require or entail a fresh assessment of the Article 83(2) GDPR criteria. Neither does it require a separate process involving the assessment of matters not previously taken into account as part of the original Articles 83(2) and (1) GDPR assessments. Rather, it is a summing up of the established position with a view to determining the specific point within the proposed fining ranges that best reflects the significant features of the particular case (both aggravating and mitigating) as well as the requirement for the final amount to be effective, proportionate and dissuasive, as required by Article 83(1) GDPR.

825. The DPC has taken account of the views expressed by CSAs in the selection of the administrative fines. The DPC notes that the French SA recommended fines at the top of the proposed ranges. The DPC does not accept TikTok Ireland's submission that this comment was insufficiently reasoned for the purpose of the selection of administrative fines. The view of the French SA was clearly stated in response to the detailed analysis set out in the Draft Decision. The comment highlighted the seriousness of the infringements, the nature of the infringements, and the number of data subjects affected as grounds for forming the view.

826. The DPC has also given careful consideration to TikTok Ireland's response to the CSA Comments.

827. The DPC has decided to impose the following administrative fines:

(iii) TikTok Ireland's infringement of Article 46(1): a fine of €485 million; and

(iv) TikTok Ireland's infringement of Article 13(1)(f): a fine of €45 million.

828. The total of these fines is €530 million.

829. In having selected from within the fining ranges proposed in the Draft Decision, the specific amounts of the administrative fines to be imposed in respect of the infringements identified above, the DPC has taken account of the following:

(i) The DPC's assessment of the individual circumstances of this particular Inquiry, as summarised above;

(ii) The purpose of the administrative fines, which, as noted above, is to enforce compliance with the GDPR by sanctioning the infringements that were found to have occurred (effectiveness);

(iii) The requirement for a genuinely deterrent effect, in terms of discouraging both TikTok Ireland and others from committing the same infringements in the future (dissuasiveness);

(iv) The requirement for any fine to be proportionate and not to exceed what is necessary to achieve the stated objective. The DPC considers that the fines are proportionate to the circumstances of the case, taking into account the gravity of the infringements and all of the elements that may lead to an increase (aggravating factors) or decrease (mitigating factors) of the initial assessment as well as the significant turnover of the undertaking concerned;

(v) The views expressed by the supervisory authorities of France and Germany insofar as those views concerned the level of fine that would be necessary in order to satisfy the requirement for fines to be effective, proportionate and dissuasive;

(vi) TikTok Ireland's various submissions furnished on fining matters, including its response to the CSA Comments.

Q. Summary of Corrective Powers

830. In summary, the corrective powers that the DPC exercises are:

(i) An order pursuant to Article 58(2)(j) GDPR requiring TikTok Ireland to suspend the Data Transfers.

(ii) An order pursuant to Article 58(2)(d) GDPR requiring TikTok Ireland to bring the processing into compliance in the manner detailed in this decision.

(iii) Two administrative fines pursuant to Article 58(2)(i) GDPR of €485 million and €45 million respectively.

831. TikTok Ireland has the right of an effective remedy against this Decision, the details of which have been provided separately.

This Decision is addressed to:

TikTok Technology Limited
The Sorting Office
Ropemaker Place
Dublin 2
D02 HD23

Decision-Makers for the Data Protection Commission:

Dr. Des Hogan
Commissioner for Data Protection

Dale Sunderland
Commissioner for Data Protection