In the matter of the General Data Protection Regulation

DPC Inquiry Reference: IN-21-9-1

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 Articles 60 and 65 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-Maker for the Commission:

[sent electronically, without signature]

Helen Dixon
Commissioner for Data Protection

Dated the 1st day of September, 2023

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

A. INTRODUCTION

1. The General Data Protection Regulation ("**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.[1]

2. The Data Protection Commission ("**DPC**" or, otherwise, "**IE SA**") 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]

3. This is a decision ("the **Decision**") of the DPC pursuant to Section 111 of the 2018 Act and Articles 60 and 65 of the GDPR. I have made this Decision, as the decision-maker for the DPC, further to an own-volition Inquiry conducted by the DPC pursuant to Section 110 of the 2018 Act ("the **Inquiry**"), concerning the compliance or otherwise of TikTok Technology Limited with its obligations pursuant to Articles 5, 12, 13, 24 and 25 GDPR in the context of the TikTok platform. For the purpose of this Decision, "**TTL**" will be used to refer to TikTok Technology Limited while "**TikTok**" will be used to refer to the platform itself, whether web- or application-based.

4. In preparing this Decision, the DPC has taken into account all submissions made by TTL in response to the Inquiry, as well as other relevant information received by the DPC, and public sources of information, as set out in this Decision.

5. This Decision further reflects the binding decision that was adopted by the European Data Protection Board ("the **EDPB**") pursuant to Article 65(2) of the GDPR,[3] ("the **Article 65 Decision**") which directed changes to certain aspects of the positions reflected in the draft decision that was presented by the DPC for the purposes of Article 60 GDPR ("the **Draft Decision**"), as detailed further, below. The Article 65 Decision will be published on the website of the EDPB, in accordance with Article 65(5) GDPR, and a copy of same is attached at Appendix 1 to this Decision.

6. It is important to note that this Decision, including the analysis and findings herein, is without prejudice to any other investigation and/or inquiry that may be conducted in relation to the assessment of the legal basis/legal bases relied upon for processing of the personal data of registered EU TikTok users under the age of 18 ("**Child Users**") by TTL in the context of the TikTok platform.

B. SUMMARY OF FACTUAL BACKGROUND

7. TikTok is a video-focused social media platform that allows registered users to create and share videos of varying durations and to communicate with other users through messages. TTL states that TikTok is not a "*social network*" and is, rather, a "*a global entertainment platform that, at its core, was designed to enable Users to create and share video content, enjoy videos from a*

[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] SI 175/2018 Data Protection Act 2018 (Establishment Day) Order 2018.
[3] Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR) (adopted 2 August 2023).

variety of creators, and otherwise express their creativity, such as by interacting with videos to express new perspectives and ideas."[4]

8. Per TTL's Director's Report and Financial Statement for the year ending 31 December 2020, TTL is a private company limited by shares, incorporated on 12 October 2018.[5] TTL's sole shareholder is TikTok Information Technologies UK Limited. TTL's ultimate parent is ByteDance Ltd.[6]

9. TikTok launched on the worldwide market in September 2017. With effect from 29 July 2020, the data controller for EU/EEA users transferred from TikTok Inc. to TikTok Information Technologies UK Ltd. and TTL as joint controllers.[7]

10. The TikTok platform is accessible via a standalone mobile phone application and can also be viewed as a webpage from a web browser. Persons who have not registered as a TikTok user can view certain content on the webpage version of the TikTok user's profile page, which is also presented in the 'For You' TikTok homepage. Access to the mobile phone application is restricted to registered users.

11. During the period of 29 July 2020 to 31 December 2020, TTL processed personal data in the context of the activities of a single establishment of a controller or processor in the European Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.[8] TTL's single establishment in Ireland is supported by affiliated entities in the European Union in Germany, France, Poland, Italy, Spain and Sweden.[9]

12. The TikTok service is provided on the basis of a written contract between TTL and the user, referred to as its 'Terms of Service'.[10] The relevant version of the Terms of Service, for the purpose of this Decision, is that of July 2020.[11]

13. The collection and use of TikTok users' personal information is described in the TikTok Privacy Policy.[12] The relevant version of the Privacy Policy, for the purpose of this Decision, is that of July 2020.[13] TikTok also has a 'TikTok Summary for Users U18'.[14]

14. Per TikTok's Terms of Service, users of the platform must be at least 13 years of age.[15] TikTok has a content rating on the Apple App store of '12+' and on the Google Play store of 'Parental Guidance Recommended'.[16] In order to register as a user of TikTok, a potential user can do so

---

[4] Response to the PDD at [3.1]-[3.2].
[5] This same information appears in TTL's Director's Report and Financial Statement for the year ending 31 December 2021.
[6] TikTok Technology Limited, 'Director's Report and Financial Statement' (Year Ending 31 December 2020). This same information appears in TTL's Director's Report and Financial Statement for the year ending 31 December 2021.
[7] Notice of Commencement at [5] and Response to the Notice of Commencement at [6.1].
[8] Response to the Notice of Commencement at [7.1].
[9] Response to the Notice of Commencement at [8.2].
[10] TTL TikTok Terms of Service.
[11] See Response to the Notice of Commencement at [4.1.1.].
[12] TTL TikTok Privacy Policy.
[13] See Response to the Notice of Commencement at [4.1.3].
[14] TTL TikTok Summary for Users U18.
[15] Response to the Notice of Commencement at [1.5] and TikTok, 'Terms of Service' (July 2020) at [2].
[16] Response to the Notice of Commencement at [1.5].

via the mobile phone application or the website and must pass through a registration process, including age verification.

C. COMMENCEMENT AND SCOPE OF INQUIRY

C.1 The Inquiry

15. The DPC has, since January 2021, been engaging with TTL in a supervisory capacity in relation to its processing of personal data of users, in particular users under the age of 18, in the EEA, for the purpose of monitoring compliance with the GDPR and the 2018 Act.

16. On 13 April 2021, the Dutch supervisory authority requested the DPC to provide mutual assistance in accordance with Article 61 GDPR by commencing a statutory inquiry to assess alleged breaches of the GDPR concerning TTL's processing of personal data of children, as examined in an "ex officio" investigation carried out by it that was commenced prior to 29 July 2020.

17. On 28 May and 5 July 2021 respectively, the French supervisory authority ("the **CNIL**" or, otherwise, "**FR SA**") requested the DPC to provide mutual assistance in accordance with Article 61 GDPR by commencing a statutory inquiry in respect of the CNIL's investigation that was commenced prior to 29 July 2020 concerning the processing of personal data (including that of children) from an online investigation of the TikTok app and website.

18. On 7 April 2021, the DPC received a submission from Stichting Onderzoek Marktinformatie, outlining concerns regarding the processing of personal data by TTL and requesting that the DPC investigate certain activities of TTL in connection with alleged infringements of the GDPR and risks for Child Users.

19. The DPC commenced an own-volition inquiry pursuant to Section 110(1) of the 2018 Act to examine the processing of personal data of Child Users by TTL in the context of the TikTok platform. The DPC notified TTL of the commencement of the Inquiry on 14 September 2021 ("the **Notice of Commencement**"). The Notice of Commencement set out the factual background to the Inquiry, the Inquiry Procedure and the issues for determination.

20. TTL responded to the queries raised by the DPC in the Notice of Commencement on 26 October 2021, enclosing a number of documents ("the **Response to the Notice of Commencement**"). On 7 February 2022, the DPC raised a number of further queries arising from TTL's response of 26 October 2021. TTL responded to this on 21 February 2022 (the "**Response dated 21 February 2022**").

21. On 3 March 2022, the DPC provided TTL with a statement of issues, wherein the DPC set out its understanding of the relevant factual background and identified the matters for determination pursuant to the GDPR ("the **Statement of Issues**"). TTL made submissions in respect of the Statement of Issues on 14 April 2022 (the "**Submissions dated 14 April 2022**").

22. On 7 June 2022, the DPC issued to TTL a Preliminary Draft Decision ("the **PDD**"), to which TTL responded by way of submissions furnished on 2 August 2022 ("the **Response to the PDD**").

23. As a result of the content of that response, the DPC made further queries of TTL on 11 August 2022, to which TTL responded on 22 August 2022.

24. On 1 September 2022, the DPC indicated to TTL that it would shortly circulate the Draft Decision to other concerned supervisory authorities for their views.[17]

25. On 2 September 2022, TTL responded stating that, as the Article 60 process was to shortly commence, it intended to submit expert evidence. At no point prior to this correspondence had it been indicated that TTL intended to make any further submissions nor was any explanation provided as to why the report did not accompany TTL's earlier submissions, in line with the procedures of the Inquiry. TTL provided its expert evidence on 7 September 2022, in the form of a report (of the same date) from Prof. Alice E. Marwick ("the **Marwick Report**").

26. The DPC finalised the Draft Decision, taking into account the Response to the PDD, the additional responses furnished by TTL on 22 August 2022 and the Marwick Report. The resulting Draft Decision was circulated to the supervisory authorities concerned (the "**CSAs**", each one being a "**CSA**") on 13 September 2022 for their views, in accordance with 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 CSAs 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:

    (a) The Italian SA raised an objection on 10 October 2022; and

    (b) The Berlin SA (representing the views of the SAs of Berlin and Baden-Württemberg) raised an objection on 11 October 2022.

27. In addition, the following comments were exchanged:

    (a) The Hungarian SA exchanged a comment on 10 October 2022;

    (b) The Danish SA exchanged a comment on 11 October 2022;

    (c) The Dutch SA exchanged a comment on 11 October 2022;

    (d) The French SA exchanged a comment on 11 October 2022; and

    (e) The Berlin SA exchanged a comment on 11 October 2022.

28. Having considered the matters raised, the DPC, by way of a composite response memorandum dated 23 December 2022, set out its responses together with the compromise positions that it proposed to take in order to give effect to the views that had been expressed by the CSAs in the various objections and comments. Ultimately, it was not possible to reach consensus with the CSAs on the subject-matter of the objections and, accordingly, the DPC determined that it would not follow them. That being the case, the DPC referred the objections to the EDPB for determination pursuant to the Article 65(1)(a) dispute resolution mechanism. In advance of doing so, the DPC invited TTL to exercise its right to be heard on all of the material that the DPC proposed to put before the EDPB. TTL exercised its right to be heard by way of its submissions dated 18 April 2023 ("the **Article 65 Submissions**").

29. Having assessed the objections, the EDPB adopted its Article 65 Decision on 2 August 2023 and notified it to the DPC and all other CSAs on 4 August 2023. Further to Article 65(2) GDPR, the

[17] Initially this erroneously stated 4 September 2022 but was clarified thereafter.

Article 65 Decision is binding upon the DPC (and all CSAs). Accordingly, and as required by Article 65(6) GDPR, the DPC has now amended its Draft Decision, by way of this Decision, in order to take account of the EDPB's determination of the objections which it deemed to be "relevant and reasoned" for the purpose of Article 4(24) GDPR. This Decision identifies, below, the amendments that were required to be made to the positions and/or findings proposed by the Draft Decision for the purpose of achieving compliance with the Article 65 Decision. For the avoidance of doubt, this Decision does not reference, or engage with, any objections which the EDPB determined either to be: (i) not "relevant and reasoned"; or (ii) not requiring of any action to be taken on the part of the DPC.

30. Prior to the finalisation and adoption of this Decision, the DPC invited TTL to exercise its right to be heard in relation to any matters in relation to which the DPC was required to exercise its own discretion or, otherwise, where an additional determination was required to be made. TTL exercised its right to be heard on such matters by way of its final submissions dated 25 August 2023 ("the **Final Submissions**"). As part of this exercise, the DPC engaged with TTL in relation to a small range of non-material amendments that it proposed to make to the Draft Decision for the purpose of taking "due account" of the views that were expressed by various CSAs in the form of comments that were exchanged with the DPC during the course of the Article 60(3) GDPR consultation period. For the avoidance of doubt, such amendments sought to address any matters which the CSAs identified as requiring clarification. While TTL, as part of its Final Submissions, has sought to characterise this exercise as one whereby the DPC has attempted to "supplement its reasoning", I am satisfied that this assertion is verifiably ill-founded. For the avoidance of doubt, I took account of all matters that were included in the Final Submissions when finalising this Decision prior to its adoption, including the correction of any identified typographical errors.

C.2 Temporal Scope of the Inquiry

31. As set out in the Notice of Commencement, the temporal scope of this Inquiry is limited to the processing of personal data by TTL during the period between 31 July 2020 and 31 December 2020 ("the **Relevant Period**").

C.3 Material Scope of the Inquiry

32. This Inquiry concerns the processing by TTL of personal data of registered Child Users of the TikTok platform and whether or not TTL has complied with its obligations under the GDPR as data controller. The 2018 Act provides that the term "child" in the GDPR is to be taken as a reference to a person under the age of 18 years. TTL provides the TikTok platform to persons over the age of 13. As a result, the term 'Child Users' in this Decision should be taken as a reference to registered TikTok users who are aged between 13 and 17 years old.[18] As set out below, this Inquiry also examines certain issues regarding TTL's processing of personal data relating to children under the age of 13.

33. In particular, this Inquiry concerns two distinct sets of processing operations by TTL in the context of the TikTok platform, both of which constitute the processing of personal data as defined by Article 4(2) GDPR. The Inquiry also examines the extent to which TTL complies with its transparency obligations under the GDPR.

[18] In its various submissions, TTL has used the term 'younger User' and in other documents refers to 'Children Users'. For the sake of consistency, the term 'Child Users' will be used throughout.

34. Broadly, the first type of processing to be examined relates to the processing of Child Users' personal data in the context of the platform settings of the TikTok platform, both mobile application- and website-based, in particular public-by-default processing of such platform settings in relation to Child Users' accounts, videos, comments, 'Duet' and 'Stitch', downloading and 'Family Pairing'.

35. The second type of processing to be examined relates to the processing by TTL of the personal data of children under the age of 13 in the context of the TikTok platform, both mobile application- and website-based, in particular for the purposes of age verification.

36. Finally, with regard to the processing of personal data of persons under the age of 18 in the context of the TikTok platform (including any such processing in connection with websites or applications which provide access to the TikTok platform), this Inquiry also examines if TTL has complied with its obligations to provide information to data subjects in the form and manner required by Articles 12(1), 13(1)(e), 13(2)(a), 13(2)(b), and 13(2)(f) GDPR.

C.4 Assessment of TTL's Compliance with the GDPR and Corrective Powers

37. The Statement of Issues identified the matters for determination as part of the within Inquiry. These issues concern TTL's compliance with the GDPR (and consideration of corrective powers), as follows:

38. Firstly, in relation to platform settings:

- *Whether, having regard to the default public settings applied to Child Users' accounts, [TTL] implemented appropriate technical and organisational measures pursuant to Article 24 GDPR to ensure and to be able to demonstrate that its processing of Child Users' personal data was performed in accordance with the GDPR;*

- *Whether, having regard to the default public settings applied to Child Users' accounts, [TTL] complied with its obligations under Article 5(1)(c) and 25(1) GDPR to ensure that its processing of Child Users' personal data was adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed; and to implement appropriate technical and organisational measures designed to implement the data minimisation principle 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;*

- *Whether, having regard to the default public settings applied to Child Users' accounts, [TTL] complied with its obligation under Article 25(2) GDPR to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed;*

- *Whether, in circumstances where [TTL's] platform settings allowed an unverified non-Child User to access and control a Child User's platform settings, [TTL] complied with its obligations under Articles 5(1)(f) and 25(1) GDPR to ensure that its processing of Child Users' personal data was processed in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and to implement appropriate technical and organisational measures designed to implement the integrity and confidentiality principle 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.[19]

39. Secondly, in relation to age verification:

- *Whether, having regard to [TTL's] requirement that users of TikTok should be aged 13 and above, [TTL] complied with its obligation under Article 24 GDPR to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that its processing its processing of personal data of Child Users was performed in accordance with the GDPR, including by implementing measures to ensure against children aged under 13's access to the platform;*

- *Whether, having regard to [TTL's] requirement that users of TikTok should be aged 13 and above, [TTL] complied with its obligations under Article 5(1)(b), 5(1)(c) and 25(1) GDPR to ensure that it collected Child Users' personal data for specified, explicit and legitimate purposes and that it did not further process that data in a manner incompatible with those purposes; to ensure that its processing of Child Users' personal data was adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; and to implement appropriate technical and organisational measures designed to implement the purpose limitation and data minimisation principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects, including by implementing measures to ensure against children aged under 13's access to the platform;*

- *Whether, having regard to [TTL's] requirement that users of TikTok should be aged 13 and above, [TTL] complied with its obligation under Article 25(2) GDPR to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed, including by implementing measures to ensure against children aged under 13's access to the platform.*[20]

40. Thirdly, in relation to transparency:

- *Whether Child Users are appropriately made aware as a user of […] TikTok of the various public and private account settings in accordance with Articles 5(1)(a), 12(1), 13(1)(e), 13(2)(a) and 13(2)(f); to be read in conjunction with Recitals 38, 39, 58, 60 and 61, and whether Child Users are able to determine the scope and the consequences of registering as a user, whether public or private;*

- *Whether Child Users are appropriately made aware as a user of […] TikTok of the public default setting in accordance with Articles 5(1)(a), 12(1), 13(1)(e), 13(2)(a) and 13(2)(f); to be read in conjunction with Recitals 38, 39, 58, 60 and 61, and whether Child Users are able to determine the scope and the consequences of registering as a user, and specifically that their profile will be defaulted to public*[21]

41. The individual assessment of these issues in light of the legal regime and TTL's submissions is set out in detail for each below.

[19] Statement of Issues at 9.
[20] Statement of Issues at 11.
[21] Statement of Issues at 13.

D. PRELIMINARY LEGAL AND PROCEDURAL ISSUES

D.1 Competence of the DPC as Lead Supervisory Authority

42. I have considered whether the processing which is the subject of the Inquiry is cross-border processing under the GDPR, and if so, whether the DPC is competent to act as lead supervisory authority in respect of the processing carried out by TTL.

43. Cross-border processing is defined in Article 4(23) GDPR as meaning 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 processer in the Union where the controller or processer 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.*

44. The TikTok Community Guidelines (April 2020 – November 2020) state that:

> *TikTok's mission is to inspire creativity and bring joy. We are building a global community where users can create and share authentically, discover the world around them, and connect with others across the globe.*

45. The TikTok Community Guidelines (December 2020) similarly provide that:

> *TikTok's mission is to inspire creativity and bring joy. We are building a global community where people can create and share, discover the world around them, and connect with others across the globe.*

46. This Inquiry pertains to social network activities of Child Users of TTL, which can involve the sharing of information with users globally. Based on the information provided by TTL and information publicly available in the Community Guidelines, I am satisfied that the subject-matter of the Inquiry concerns the cross-border processing of personal data, within the meaning of Article 4(23) GDPR.

47. Turning to the question of whether the DPC is competent to act as lead supervisory authority in respect of the processing under examination, I note that Article 56(1) GDPR provides that the supervisory authority of the "*main establishment*" of a controller or processor shall be competent to act as *"lead supervisory authority*" pursuant to Article 60 GDPR.

48. TTL is a private company limited by shares having its registered office at 10 Earlsfort Terrace, Dublin 2, Ireland. TTL's Terms of Service state that:

> *TikTok is a leading platform for creating and sharing short-form videos (the "Platform"). You are reading the terms of service (the "Terms"), which govern the relationship and serve as an agreement between you and us and set forth the terms and conditions by which you may access and use the Platform and our related websites (such as tiktok.com), services, applications, products and other content which are stated to be offered subject to these Terms (collectively, the "Services").*

The Services are provided by the company that offers the Services in your region ("TikTok", "we" or "us"):

Residents of the EEA + Switzerland: The Services are provided by TikTok Technology Limited, which is registered in Ireland with its registered office at 10 Earlsfort Terrace, Dublin, D02 T380, Ireland and company number 635755.

49. In its Response to the Notice of Commencement , TTL confirmed that the TikTok platform is a video-focused platform for which, with effect from 29 July 2020, the data controller for EU/EEA users transferred from TikTok Inc. to TikTok Information Technologies UK Ltd. and TTL as joint controllers.[22]

50. Having considered all of the above and the nature of the processing at issue, I am satisfied that TTL is a data controller (within the meaning of Article 4(7) GDPR) with regard to the processing which is the subject of this Inquiry. I am further satisfied that TTL has its main establishment in Ireland for the purposes of the GDPR. As such, I am satisfied that the requirements of Article 56 GDPR have been met in relation to the processing at issue, such that the DPC is competent to act as the lead supervisory authority in respect of the cross-border processing under examination.

D.2 Approach to the examination of compliance

51. TTL contends that, were its approach to compliance to be assessed by reference to the DPC's "Fundamentals for a Child-Oriented Approach to Data Processing" (published December 2021) ("the **Fundamentals**"),[23] which were not issued until after the Relevant Period, this would constitute *"an impermissible retrospective application of regulatory standards and a clear breach of fair procedures"*.[24]

52. The Fundamentals is a guidance document resulting from three separate stakeholder consultation processes, including a direct consultation with children, engagement with experts in the area of children's rights, expansive research and a two-stage drafting process. As part of the drafting process, the DPC sought the views of adult stakeholders including parents, educators, children's rights organisations and industry, amongst others, on core data protection issues pertaining to children by means of a traditional online consultation document and then engaged directly with children and young people in the classroom through a specially designed consultation process.

53. Following several months of in-depth academic and policy research and legal analysis, as well as further engagement with key stakeholders in the area of children's rights, in December 2020, the DPC published a draft version of the Fundamentals and ran a public consultation on the document between 18 December 2020 and 31 March 2021, to give stakeholders a final opportunity to present their views. In total, 27 submissions were received in response to this consultation. Participating stakeholders came from a wide range of sectors, including technology and social media companies, children's rights charities, public sector bodies and trade associations. A detailed report on the submissions received in response to this public consultation was published in November 2021, along with the DPC's responses to the various thematic issues which emerged.

---

[22] Notice of Commencement at [5] and Response to the Notice of Commencement at [6.1].

[23] Accessible via https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

[24] Submissions dated 14 April 2022 at [13].

54. The Fundamentals introduces child-specific data protection interpretative principles and recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their use of/ access to services in both an online and offline world. The Fundamentals will also assist organisations that process children's data by clarifying the principles, arising from the high-level obligations under the GDPR, to which the DPC expects such organisations to adhere.

55. From December 2021, the Fundamentals had immediate application and operational effect, now forming the basis for the DPC's approach to supervision, regulation and enforcement in the area of processing of children's personal data.

56. While it is accepted that the finalised Fundamentals post-dates the Relevant Period, I note that the GDPR does not depend on ancillary guidance documents for its legal application; TTL was obliged to comply with the GDPR since May 2018, without the need for additional legislative guidance. It is an inherent feature of the GDPR that its provisions are not prescriptive. I do not accept that reference to principles derived from the GDPR could constitute an impermissible retrospective application of regulatory standards and a clear breach of fair procedures and, in fact, to do so would be entirely self-defeating.

57. However, it is accepted that it would be deleterious to TTL's entitlement to fair procedures to determine its compliance by reference to guidance set out in the Fundamentals that arose as a result of the development of the Fundamentals itself. Accordingly, this Decision will assess TTL's compliance by reference to the GDPR itself and guidance and materials that were available during the Relevant Period. Following the provision to TTL of the PDD, no further submissions in this regard were made by TTL.

E. ASSESSMENT OF CERTAIN MATTERS CONCERNING ARTICLES 5, 24 AND 25 GDPR

E.1 Nature, Scope, Context and Purpose of the Processing

58. This Decision assesses TTL's compliance with Articles 24 and 25 GDPR with regard to the processing described above. Articles 24 and 25 GDPR expressly require the taking into account of the *"nature, scope, context and purposes"* of the processing. I have therefore considered each of these four criteria, in order to inform the subsequent analysis of the above three provisions of the GDPR in the Decision, as follows:

Nature of the processing

59. The nature of processing refers to the basic or inherent features of the processing operations performed on personal data by a data controller. This Decision relates to two types of processing by TTL: public-by-default processing of Child Users' social media content and the processing of personal data of children under the age of 13 in the context of the TikTok platform, both mobile application- and website-based, in particular for age verification purposes.

Scope of the processing

60. The scope of processing refers to the extent of operations performed on personal data by TTL. TTL has stated that, during the period of 29 July 2020 to 31 December 2020, the approximate total average number of registered EU TikTok users under the age of 18 was [redacted]. The

approximate total average number of monthly EU TikTok users under the age of 18 was [redacted].[25]

61. TTL has stated that it does not retain personal data to determine the approximate number of TikTok users that were identified as being under the age of 13 when attempting to register during the period from 29 July 2020 to 31 December 2020; however, TTL believes that the approximate number of individuals in the EU who were failed registration on the basis of their identifying as an individual below 13 years of age during the equivalent number of days from 14 April to 16 September 2021 was [redacted].[26] During the period of 29 July 2020 to 31 December 2020, the approximate number of EU TikTok users that were detected as being under 13 subsequent to their registration and removed from the platform was [redacted].[27]

62. TTL does not hold statistics on users' account status beyond [redacted] however, the approximate daily average number of EU TikTok users under the age of 18 with a private account at 23:59 hours on a given day between 14 September 2021 to 14 October 2021 was [redacted].

63. TTL does not retain information on the approximate number of persons under the age of 18 that operated a public TikTok account during the period from 29 July 2020 to 31 December 2020; however, the approximate daily average number of EU TikTok users under the age of 18 with a public account at 23:59 hours on a given day between 14 September 2021 to 14 October 2021 was [redacted].[29]

64. With regard to the scope of the public-by-default processing, by setting accounts of newly registered users of TikTok to public by default whereby, unless the Child User opted for a private account, TTL created the conditions whereby the social media posts and content of Child Users would be shown to a global audience of millions of other TikTok users, and persons off-TikTok, via its website. Accordingly, by setting accounts to public by default, TTL ensured that the scope of processing social media content of Child Users was potentially very extensive, being made accessible without restriction to an indeterminate global audience.

65. With regard to the scope of the processing of the personal data of children under 13, TikTok has indicated that, during the period of 29 July 2020 to 31 December 2020, the approximate number of EU TikTok users that were detected as being under 13 subsequent to their registration and removed from the platform was [redacted]. The number of children under 13 who used the TikTok platform and were not detected is unknown. Accordingly, TTL processed the personal data of at least approximately this number of children under 13 and, by setting accounts to public by default, TTL ensured that the scope of processing of social media content of children under 13 was potentially very extensive, being made accessible without restriction to an indeterminate global audience.

Context of the processing

66. The context of processing refers to the circumstances that form the setting of the processing.

---

[25] TTL initially indicated this number was [redacted] in Response to the Notice of Commencement at [9.2.1]-[9.2.2.]; however, in Submissions dated 14 April 2022 at Annex A, it revised this downward to take into account users who turned 18 during the Relevant Period.
[26] Response to the Notice of Commencement at [9.2.3].
[27] Response to the Notice of Commencement at [9.2.4].
[28] Response to the Notice of Commencement at [9.2.5].
[29] Response to the Notice of Commencement at [9.2.6].

67. This Inquiry relates to both registered TikTok users who are at least 13 years old, and younger than 18 years old, as well as children under 13. The GDPR recognises children as a vulnerable category of people and, in particular, Recital 38 GDPR notes that children *"merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data"*.

68. In terms of the context in which accounts of Child Users are set to "public" by default on registration, TTL states that:

> *"To promote the fact that Users could select a private account at any time, at the time of registration, Users between the ages of 13-17 ("under 18 Users") were presented with a full-screen pop-up notification highlighting account privacy, explaining, at a high-level, what a private account involved, and the implications of having a public account setting. This notice comprised a pro-privacy nudge containing a prominent button which Users could press to "Go Private", and also reminded under 18 Users that they could change their privacy settings at any time in the app settings. Steps were therefore taken to empower younger Users to make an informed decision about their account setting. In this respect, it is also worth recalling that, by design, TikTok is a platform which is designed to enable users to share video content that they create. Younger Users may therefore have specific and legitimate reasons to want to have a public account, such as where they are seeking to build a wider following for their content. Given this, the pro-privacy nudge approach was an appropriate means to encourage younger Users to actively engage with their relative privacy settings adopted during the Relevant Period."*[30]

69. It is a common expectation of social media users that they will have control over who sees their content.[31] This well-established expectation of audience control is reflected in TTL's decision to implement a private account setting. It is very clear that although many TikTok users have adopted the platform as a place to "*build a wider following for their content*", others prefer to limit the sharing of their posts to a controlled audience of followers. The expectations of users will vary from the outset depending on how they want to use the service, and may change over time.

70. While TTL has provided a pop-up notification at the point of registration, querying whether the user wishes to opt for a private account, users must positively opt to do or may 'skip' this decision and their account is made public-by-default.[32] TTL has not opted to invert this choice whereby Child Users' or users' accounts would be set as private-by-default and users would actively intervene either at the point of registration or later to opt to make their profiles public. This public-by-default setting appears to be a deliberate choice on the part of TTL, intended to maximise user engagement and sharing on the platform.

71. While, of course, as TTL states, Child Users may have *"specific and legitimate reasons to want to have a public account, such as where they are seeking to build a wider following for their*

---

[30] Response to the Notice of Commencement at [10.2].

[31] For example, see Commission Nationale de l'Informatique et des Libertés, 'Les comportements digitaux des enfants' (February 2020) at 24, accessible via https://www.cnil.fr/sites/default/files/atoms/files/sondage_ifop_-_comportements_digitaux_des_enfants_-_fevrier_2020.pdf

[32] Response to the Notice of Commencement and Image 1.

content", it is not clear how such legitimate or specific reasons would be undermined by inverting such a choice, or defaulting the account to private.

72. TTL also states that "*TikTok is a platform which is designed to enable Users to express their creativity through the sharing of their video content and interaction with other User's content.*"[33] Insofar as it could be said that private-by-default would adversely affect this, users with private accounts are not limited in what they can see on the platform, and the existence of a user's profile is public and searchable, thereby facilitating easy connection and the sharing of content with approved followers.

73. Content shared publicly on TikTok is not limited to registered users. Such content is also made available on the web browser version of a profile page to an indeterminate global audience of persons who are not registered users. Certain content on the web browser version can be seen by anyone without logging in as a registered member.

74. In its Response to the PDD, TTL disputed that there was public-by-default processing at all.[34] This was the first time this submission was made, and contrasted to the previous submissions made following the Statement of Issues, for example those excerpted above.[35] Indeed, this submission is also inconsistent with other statements that TTL has made in this regard.[36] In any event, in the premises, it is not accepted that, as a matter of fact, an account is not public-by-default. As set out above, users must positively opt for a private account – this is a choice that they must make in order to avail of it or they may simply chose to 'skip' this decision, in which case their account is public-by-default.

75. In this regard, I note that the EDPB's Guidelines 4/2019 on Article 25 Data Protection by Design and by Default state that:

> *Fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes).*
>
> *Key design and default fairness elements may include:*
>
> [...]

---

[33] Submissions dated 14 April 2022 at [32].

[34] Per Response to PDD at [3.3]-[3.7], [5.3]-[5.5], [5.32], [5.62], [5.80]-[5.88], *inter alia.*

[35] Response to the Notice of Commencement at [10.2].

[36] See, for example, TTL, 'Curating your following' (13 November 2019), accessible via https://newsroom.tiktok.com/en-us/curating-your-following and TTL, 'Controlling what people see on your profile' (9 May 2019): , accessible via https://newsroom.tiktok.com/en-us/post-7-controlling-what-people-see-on-your-profile: "*By default, your account starts as public, which means any TikTok user can view your videos and post comments, reactions, or duets to engage with the content you've created and shared – but you can easily change this in your Privacy Settings*".

- *No deception – Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.*[37]

76. The language utilised – to 'skip', that is, to omit, bypass or leave out – plainly means that, without purposefully making this decision, the account would be public. Therefore, the default setting, absent a user selecting the private account, is a public account. Indeed, if this were not the case, then there would be nothing as such to 'skip'. It is not sustainable to state this does not constitute public-by-default.

77. In the Response to the PDD, TTL states that: "*The PDD makes a number of references to younger Users having to "opt" for a private account. See, for example, paragraphs 61, 67, 121, 140, 150 and 219 of the PDD. However, the logical converse of this statement is that younger Users would also need to "opt" for, i.e. choose, a public account.*" This is a very artificial understanding of the use of the term 'opt', which has actually been used to refer to positive decisions that a user must make in order to avail of a private account, or omit this decision rendering the account public-by-default.[38]

78. The use of the language employed, as well as the fact that the platform settings did not employ the inverse of the available selection – that is, the pop-up notification seeking the user's intervention to 'Go Public' rather than to 'Go Private' or, for example, the accounts of under-16 users being set to private, without any ability to skip this during the registration process – all demonstrate that the account was public-by-default. Therefore, having considered TTL's Response to the PDD in this regard in full, as well as all other responses and materials, I am of the opinion that the processing is public-by-default for these reasons. I have set out, below, my consideration of the lawfulness of TTL's processing, in this regard.

Purposes of the processing

79. The purpose of processing refers to the reasons for processing personal data. In connection with TTL's decision to make social media posts of Child Users publicly visible by default, TTL states that:

> *TikTok is a global entertainment platform that, at its core, is designed to enable Users to create and share video content. The primary purpose of the Platform during the Relevant Period was not to connect a User with other Users (in contrast to other platforms), but rather to enable Users to disseminate their own content and to show Users content that they would likely find of interest. This enabled Users to express themselves in a creative and engaging way and to participate in multi-cultural engagement, discovering new perspectives, ideas and inspiration.*
>
> *During the Relevant Period, Users would have understood when they registered for the Platform that its purpose was to enable them to create and share videos with, and enjoy videos from, a variety of creators, and otherwise express their creativity, including by interacting with videos of other Users to express new perspectives and*

[37] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, (20 October 2020) at [69]-[70], accessible via https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

[38] Response to the PDD at [3.6] and Footnotes 13 and 40.

ideas. This would have informed Users' (including younger Users') expectations in connection with the Platform and the processing of their personal data.[39]

And:

As explained above, TikTok's mission is to inspire creativity and bring joy. The core nature of the Platform during the Relevant Period was to show Users content they were likely to find of interest, regardless of which user created it, and to enable Users to disseminate their own content. Users understood when they registered for the Platform during the Relevant Period that its purpose was to enable them to create and share videos with, and enjoy videos from, a variety of creators, and otherwise to express their creativity, such as by interacting with those videos to express new perspectives and ideas. [...][40]

80. In my view, this default processing arrangement by TTL also serves the purpose of prompting wider and more extensive sharing of user content which, in turn, promotes user engagement with the service and, therefore, advances the commercial interests of TTL.

E.2 Risks of varying likelihood and severity resulting from the processing

81. Articles 24 and 25 GDPR require data controllers to take into account the risks (of varying likelihood and severity) for the rights and freedoms of natural persons posed by processing of personal data, and to implement measures and safeguards that apply data protection principles and protect the rights of data subjects. I have therefore considered the risks posed by TTL's processing of Child Users' personal data, and the measures and safeguards implemented by TTL in response.

82. Recital 75 GDPR provides examples of risks to the rights and freedoms of natural persons. These risks may include physical, material or non-material damage to natural persons. In particular, Recital 75 specifies the following relevant risks to the rights and freedoms of natural persons:

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 the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

[39] Submissions dated 14 April 2022 at [8]-[9].
[40] Submissions dated 14 April 2022 at [27].

83. Recital 76 GDPR further outlines how a risk assessment is to be carried out by a controller, as follows:

> *"The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."*

84. The EDPB has stated that:

> *"29. The GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing).*
>
> *30. When performing the risk analysis for compliance with Articles* [sic] *25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments.*
>
> [...]
>
> *32. ... controllers ... must always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed. ..."*[41]

85. By way of its Submissions dated 14 April 2022, TTL states that:

> *TikTok has also provided the DPC with the DPIAs which cover the processing activities undertaken on U18 Data. These DPIAs demonstrate how TikTok implemented appropriate technical and organisational measures on the Platform, including in circumstances where younger Users chose not to exercise the option during account registration to select a private account, to ensure that its processing of U18 Data was performed in accordance with the GDPR.* ***Specifically, the public account setting had been addressed in the following DPIAs: Children's Data and Age Appropriate Design DPIA, User Safety & Content Moderation DPIA, Content Publication & Engagement DPIA, Content Personalisation & Recommendation DPIA, Personalised Ads DPIA, and Generic Ads DPIA.*** *For example, the Children's Data and Age Appropriate Design DPIA addresses how the risk with social media audience reach is mitigated on the Platform.*[42] (emphasis added)

[41] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and Default (20 October 2020).

[42] Submissions dated 14 April 2022 at [73].

86. In relation to the Relevant Period, TTL has conducted a data protection impact assessment in relation to Children's Data and Age Appropriate Design of 8 October 2020 ("the **DPIA**"). While TTL identifies a number of other data protection impact assessments, this is the most relevant.

87. Schedule 2 to the DPIA sets out the risks identified, a description of the risk, an assessment of the risk level before any mitigations are put in place ("**Inherent Risk**"), the proposed mitigation measures to be put in place, and an assessment of the risk level after the relevant mitigations have been put in place ("**Residual Risk**"). The methodology for calculating the overall risk score for each risk is as follows: [redacted] This is applied for both the Inherent Risk and the Residual Risk.

88. The DPIA identifies thirteen risks to Child Users. These are:

(a) [redacted]
(b) [redacted]
(c) [redacted]
(d) [redacted]
(e) [redacted]
(f) [redacted]
(g) [redacted]
(h) [redacted]
(i) [redacted]
(j) [redacted]
(k) [redacted]
(l) [redacted]
(m) [redacted][43]

89. TTL identifies the [redacted] In relation to its mitigation measures including, as appropriate, the platform settings, TTL determines that the [redacted] TTL concludes:

[redacted]

[43] The DPIA at Part B, Schedule 2.

[redacted]

90. In its Response to the PDD, TTL states:

> *In particular, it is unclear how access to video content "off-TikTok", which we understand to mean access by unregistered users of the TikTok website, creates a greater risk than where such content is accessed on the Platform.*
>
> *More generally, TikTok considers that the DPC's focus on "loss of control" as a category of harm suffered by younger Users is incorrect. TikTok notes that recital 85 GDPR refers to the "loss of control" as an example of damage that may flow from a personal data breach: This clearly refers to a loss of control by reason of a data breach; there was no personal data breach in this case and "loss of control" is not an expression used elsewhere in the GDPR. "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned"* (emphasis added).[45]

91. Insofar as this Inquiry relates to public-by-default processing, were a Child User to avail of the relevant public features of the TikTok platform, that could lead in the first instance to Child Users losing autonomy and control over their data and, in turn, they could become targets for bad actors, given the public nature of their use of the TikTok platform. This could also lead to a wide range of potentially deleterious activities, including online exploitation or grooming, or further physical, material or non-material damage where a Child User inherently or advertently reveals identifying personal data. There is the identified risk of social anxiety, self-esteem issues, bullying or peer pressure in relation to Child Users.

92. Insofar as this Inquiry relates to age verification platform settings, where a child under the age of 13 were to gain access to the TikTok platform, further to the risks identified in relation to public-by-default processing which apply equally, if not more severely to children under 13, such as a child under 13 may be at risk of viewing and accessing materials that are harmful or inappropriate for a child of such youth, particularly given that the TikTok platform is not intended for children under 13.

93. As well as this, generally, I also note that the processing which is at issue in this Inquiry involves the public and off-TikTok dissemination of the personal data of Child Users. While TTL has set out that it has a suite of on-platform reporting tools and safeguards which will be evaluated below, the public-by-default account setting exposes social media posts by Child Users to an indeterminate audience. This presents a severe risk for Child Users. While TTL disputes this, as set out above, the reason this is the case is that the range of reporting tools and safeguards that it has stated apply, would be largely of no use against those off-TikTok.

94. While TTL has conducted a DPIA in relation to Children's Data and Age Appropriate Design, notably this DPIA does not identify the risk of children under the age of 13 accessing the TikTok platform and the further risks that may arise from this. While the risks identified in the DPIA

[44] The DPIA at 15.
[45] Response to the PDD at [4.10]-[4.12].

apply equally to children under the age of 13 as those over the age of 13, the risks associated with these younger users is exacerbated and particularly severe given their young age and the fact that the TikTok platform is expressly not intended for those under the age of 13.

95. Further to these identified risks, it is also clear that TTL's processing of users' personal data presented risks relevant to a number of the data protection principles provided for under Article 5 GDPR. In assessing TTL's compliance with Articles 24 and 25, I must have regard to the risk of bad actors misusing the TikTok platform to acquire personal data in a manner that is deleterious to the rights and freedoms of data subjects. It is clear that this risk relates to a number of data protection principles as provided in Article 5 GDPR.

96. In this regard, the Response to the PDD stated:

> *More generally, the PDD appears to be focused on matters which go beyond TikTok's processing of younger Users' personal data. For example, the PDD analyses the risk related to compliance with the purpose limitation principle under Article 5(1)(b) GDPR based on the potential for "TTL users' personal data [being] processed in a manner that is incompatible with the purposes for which the personal data were collected." However, the DPC's main focus in the PDD appears to be the actions of third parties, namely "where the platform is used by bad actors to for the risks set out above, rather than [TikTok's] purpose, this would amount to processing of personal data in the relevant features in a manner that is incompatible with the purposes for which the personal data were collected." There is no evidence before the DPC in this Inquiry that the Platform is in fact used by bad actors in the manner suggested in the PDD. Moreover, the DPC appears to be equating the potential actions of bad actors with the processing actually carried out by TikTok and its obligations under Article 5 GDPR. It is respectfully submitted that this goes beyond the ambit of the GDPR and constitutes an error of law in the PDD.*[46]

97. The risk, for example, relates to the purpose limitation principle provided for in Article 5(1)(b) GDPR because of the potential for TTL users' personal data could be processed in a manner that is incompatible with the purposes for which the personal data were collected. The relevant features were designed to enable users to "*create and share videos with, and enjoy videos from, a variety of creators, and otherwise express their creativity, including by interacting with videos of other Users to express new perspectives and ideas*".[47] However, where the platform is used by bad actors for the risks set out above, rather than this purpose, this would amount to processing of personal data in the relevant features in a manner that is incompatible with the purposes for which the personal data were collected. With regard to TTL's above submission, the PDD does not "*focus on matters which go beyond TikTok's processing of younger Users' personal data.*" The PDD is not attributing actions of bad actors to TTL, rather it states that risk arises in relation to the platform settings with regard to the purpose limitation principle. It appears to me that TTL is suggesting that the purpose limitation principle could not give rise to an obligation to implement appropriate organisational and technical measures in the context of the potential actions of bad actors. I do not agree; TTL has a responsibility under the GDPR to implement appropriate measures to prevent the platform settings being used for a purpose other than that intended.

98. The risk also relates to the data minimisation principle provided for in Article 5(1)(c) GDPR. This principle requires that personal data shall be adequate, relevant and limited to what is

[46] Response to the PDD at [4.23].
[47] Submissions dated 14 April 2022 at [9].

necessary in relation to the purposes for which they are processed. Users may create video content on TTL and engage with the platform settings for a range of different purposes, for example, for the purposes of creating and sharing videos and connecting with friends. There is a risk that the processing on the TikTok platform may include personal data that were not collected for these purposes. Even if users may have provided their personal data to TTL for the purpose of creating and sharing videos with registered TikTok users, including friends, that is indeed entirely different to doing so in a manner that exposes these videos containing personal data to an indefinite audience.

99. Further, the risk also relates to the integrity and confidentiality principle provided for in Article 5(1)(f) GDPR. This principle requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing. TTL's platform settings are important for enabling data subjects, including Child Users, to control certain processing operations that may be applied to their personal data. For example, the settings should reflect data subjects' choices with regard to who can view their content and who can contact them via comments or direct messages. The public-by-default settings create a risk of unauthorised access to Child Users' personal data as inadvertently or advertently disclosed in video content or via comments. This could take the form of bad actors using the TikTok website to access the personal data of Child Users in a manner that cannot be moderated by TTL. Any such access to that data as a result of utilising the website in this manner would be unauthorised access. Similarly, any processing of the personal data that enabled third parties to contact Child Users by means of comments or direct messages despite the Child User choosing settings that prevented comments and direct messages, would constitute unauthorised processing.

100. In conclusion, I am satisfied that there are possible and severe risks associated with the two forms of processing which are the subject of this Inquiry; these risks are primarily related to possible communication between Child Users and dangerous individuals, both on and off the TikTok platform. Accordingly, I believe the processing at issue resulted in high risks to the rights and freedoms of Child Users, for the purpose of Articles 24, and 25 GDPR, which are addressed further in turn below.

101. Accordingly, on the basis of the issues for determination, and indeed [redacted] and referred to in its various submissions, a number of clear risks within the rubric of Recital 75 arise which could lead to physical, material or non-material damage. In particular, the processing concerns public-by-default processing of personal data of vulnerable natural persons, that is children, and where such children are below the age of 13. The processing of their data, given the high numbers of affected and potential affected users, constitutes processing involving a large amount of personal data and affecting a large number of data subjects. Per TTL's own DPIA, [redacted]

102. As a controller, TTL is obliged to identify risks which are posed by processing, as a requirement of the principle of accountability and Articles 24 GDPR and 25. Accordingly, having had regard to the nature, scope, context and purposes of processing, as well as TTL's own risk assessment set out in the DPIA [redacted] I am satisfied that both types of processing which are the subject of this Inquiry pose high

risks to the rights and freedoms of Child Users, for the purposes of Articles 24 and 25 GDPR. In conclusion, I am satisfied that the risks associated with the processing which is the subject of this Inquiry were high both in terms of likelihood and severity.

103. The appropriateness of the technical and organisational measures that were implemented by TTL as set out in its various submissions will be evaluated in detail below in relation to platform settings and age verification respectively.

F. ISSUE 1: ASSESSMENT AND CONSIDERATION OF MATTERS CONCERNING TTL'S COMPLIANCE WITH ARTICLES 5, 24 AND 25 GDPR CONCERNING ITS PLATFORM SETTINGS FOR USERS UNDER AGE THE AGE OF 18

F.1 Application of Articles 5, 24 and 25 GDPR

104. The Statement of Issues included, as matters for determination, an assessment of whether TTL has complied with its obligations under Articles 5(1)(c), 5(1)(f), 24 and 25 GDPR, regarding its platform settings.

105. Article 5(1)(c) GDPR provides that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*" Per Recital 39, this requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

106. Article 5(1)(f) provides that personal data shall be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*" Per Recital 39, personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to, or use of, personal data and the equipment used for the processing.

107. Further, Article 24(1) provides:

> *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

108. Recital 74 GDPR clarifies what is meant by 'measures' in the context of Article 24 GDPR, by emphasising that measures implemented to comply with the GDPR should be demonstrably 'effective', as follows:

> *The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take*

into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

109. Articles 25(1) and (2) GDPR provide that:

> 1. *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.*
>
> 2. *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

110. The EDPB has published Guidelines on Data Protection by Design and by Default, which summarise Article 25 GDPR as follows:

> *The core of the provision is to ensure appropriate and effective data protection both by design and by default, which means that controllers should be able to demonstrate that they have the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.*[48]:

111. Recital 78 GDPR is also relevant. It states that:

> *The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such*

[48] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020) at [2].

products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

112. The obligation to implement measures and safeguards described in Article 25(1) GDPR is referred to as Data Protection by Design.

113. The requirement of effectiveness is a key element of Article 25(1) GDPR, as set out in the EDPB guidelines:

> *Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.*
>
> *...First, it means that Article 25 does not require the implementation of any specific technical and organisational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk. Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing.*
>
> *...Second, controllers should be able to demonstrate that the principles have been maintained.*[49]

114. Article 25(2) GDPR requires data controllers to implement measures to ensure that, by default, the principle of data minimisation is respected, as follows:

> *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

115. The obligation to implement measures described in Article 25(2) GDPR is referred to as Data Protection by Default.

---

[49] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020) at [13].

116. Article 25 GDPR does not prescribe the implementation of any specific technical and organisational measures, or safeguards; the appropriate measures and safeguards must be identified by the data controller, having considered the specific processing at issue.

117. In its Response to the Notice of Commencement and Submissions dated 14 April 2022, TTL makes a number of submissions regarding the relevant articles. In relation to Article 5(1)(c) GDPR, TTL states:

> *The data minimisation principle under Article 5(1)(c) GDPR is not an absolute obligation to process the minimum personal data possible. Rather, as described by the CJEU in Latvijas Republikas Saeima, it is a principle "...according to which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and which gives expression to the principle of proportionality" (emphasis added).*
>
> *Indeed, the DPC's 'Quick Guide to the Principles of Data Protection' acknowledges that the amount of personal data that is adequate, relevant and limited in any given case needs to be assessed by controllers based on the circumstances of their intended processing operations.*[50]

118. In relation to Article 24 GDPR, TTL states:

> *Article 24(1) GDPR imposes a general obligation on controllers to "implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with" the GDPR. Such measures must "be reviewed and updated where necessary" and, where proportionate in relation to processing activities, the measures must include "the implementation of appropriate data protection policies by the controller".*
>
> *The "appropriateness" of the relevant measures are assessed "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". In other words, the appropriateness of the measure needs to be informed by the risk assessment.*
>
> *Article 24(1) GDPR is not prescriptive as to how controllers should comply with their obligations or what measures need to be put in place. Indeed, such a prescriptive approach would be inconsistent with the objective of these provisions, which is to embed privacy compliance practices into the internal practices of organisations in a manner appropriate to the processing activities undertaken by a particular organisation.*
>
> *The Article 29 Working Party ("A29WP") noted that "the type of procedures and mechanisms would vary according to the risks represented by the processing and the nature of the data" and that "...in determining the types of measures to be implemented, there is no option but "custom built" solutions. Indeed, the specific measures to be applied must be determined depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and the types of data. A one-size-fits-all approach would only force data controllers into*

[50] Submissions dated 14 April 2022 at [21]-[22].

structures that are unfitting and ultimately fail." Accordingly, the accountability obligations under Article 24(1) GDPR are non-prescriptive and open-ended.[51]

119. Further:

In accordance with Article 24 GDPR, controllers are required to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR, and to be able to demonstrate such compliance. The measures to be adopted in this regard are to be informed by an assessment of: (i) the nature, scope, context and purposes of processing; and (ii) the risks of varying likelihood and severity for the rights and freedoms of natural persons.

It is clear, therefore, that the appropriateness of the measures adopted must be informed by an assessment of the context and purposes of processing, as well as the risks which may result from the processing (if any). As explained above, TikTok's mission is to inspire creativity and bring joy. The core purpose of the Platform during the Relevant Period was to enable Users to disseminate their own content and to show Users content they are likely to find of interest. As explained in detail in paragraphs 8, 9, 17 and 27 above, Users understood when they registered for the Platform that its purpose was to enable them to create and share videos with, and enjoy videos from, a variety of creators, and to otherwise express their creativity, including by interacting with videos of other Users to express new perspectives and ideas. This would have informed and influenced younger Users' expectations through the Relevant Period and provides an important context of the processing.

The GDPR does not prescribe the exact means of achieving, or demonstrating, compliance with its requirements. Indeed, such a prescriptive approach would be inconsistent with the objective of Article 24 GDPR, which is to embed privacy compliance into the internal practices of organisations in a manner that works for each organisation while remaining aligned with GDPR principles. Article 24 GDPR is a different obligation to Article 25 GDPR, and considers data protection compliance more holistically than Article 25 GDPR, which is focused on data protection by design and by default. Nonetheless, the controls mentioned in the October 2021 Response and, in particular, those mentioned in Section 3.1.7 User privacy controls above, and the backend protections mentioned in Section 3.1.9 Backend protections above, are equally applicable for Article 24 GDPR compliance regarding the implementation of appropriate technical measures.[52]

120. In relation to Article 25 GDPR, TTL states:

Similarly to Article 24(1), Article 25(1) GDPR does not solely focus on user controlled settings as a technical measure but also addresses technical measures more broadly (including ones that are not user controlled) and organisational measures. As such, TikTok as a data controller is afforded autonomy and appropriate latitude in determining the specific designs of its product. The measures to be adopted in Article 25(1) GDPR should be commensurate with the risks posed by the processing, and those risks should be weighed by their likelihood and severity. The European Data Protection Board ("EDPB") Article 25 Data Protection by Design and Default Guidelines ("Article 25 Guidelines") recognise that Article 25(1) GDPR does not envisage a one-size fits all

[51] Response to the Notice of Commencement at [13.2]–[13.5].
[52] Submissions dated 14 April 2022 at [62]-[64].

approach to data protection. The EDPB Article 25 Guidelines further state "[w]hen performing the risk analysis for compliance with Articles 25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks." [...][53]

And also:

Article 25(2) states, among other things that "the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" (emphasis added). Article 25(2) requires that, by default, only the personal data that is necessary for each specific purpose is processed. It is the responsibility of the controller to define the purpose of the processing, and by doing so, the controller also determines the scope of the processing required for that particular purpose. Article 25(2) therefore requires implementing default settings to processing that is necessary to achieve the controller's purpose.

Article 25(2) is not prescriptive as to the type of technical and organisational measures that must be implemented to ensure data protection by default. The EDPB has recognised that a range of different measures, including enabling data subjects to intervene in the processing, could be involved "depending on the context and risks associated with the processing in question". The context of the processing is central to the consideration as to what measures are appropriate in the given circumstances and to what extent they will implement data protection principles effectively. In particular, Article 25(2) does not require controllers to choose default settings which would subvert the core functionalities of their service.[54]

In order to comply with Article 25(1) GDPR, controllers are asked to weigh a multitude of broad and abstract concepts, assess the risks, and then determine "appropriate" measures. Each of these elements is opaque and open to interpretation, and as a result, no two assessments performed in accordance with Article 25 will look the same. Article 25(1) requires "appropriate" measures, which when applied to age verification would mean that a controller is required to implement measures to determine the age of users with an appropriate, rather than absolute, level of certainty.[55]

121. Further:

Article 25(1) GDPR does not prescribe the appropriate technical and organisational measures designed to implement the data protection principles (including the data minimisation principle) that organisations are required to put in place. Controllers are similarly afforded autonomy and appropriate latitude under Article 25(2) GDPR in determining the appropriate measures for ensuring privacy by default.

The European Data Protection Board ("EDPB") in its Article 25 Data Protection by Design and by Default Guidelines ("Article 25 Guidelines") explains that "[b]eing appropriate means that the measures and necessary safeguards should be suited to achieve the intended purpose, i.e. they must implement the data protection principles

[53] Response to the Notice of Commencement at [13.6].
[54] Response to the Notice of Commencement at [13.10]-[13.11].
[55] Response to the Notice of Commencement at [15.5].

effectively" and that "the controller must verify the appropriateness of the measures for the particular processing in question".

Further, in considering whether the measures put in place by TikTok complied with Article 25(1) GDPR, account must be taken, in particular, of the "context and purposes of processing". In this regard, full consideration must be given to the benefits of the relevant features to Users and their importance to the core purpose of TikTok during the Relevant Period as described above, which would have informed younger Users' expectations, and the measures and privacy settings designed to safeguard younger Users.[56]

122. All submissions made in this respect have been fully taken into consideration.

F.2 Analysis and findings regarding TTL's compliance with Articles 5, 24 and 25 GDPR in connection with platform settings

Overview of Issues and Technical and Organisational Measures

123. Articles 24 and 25 GDPR require the implementation of technical and organisational measures in order to comply with the accountability principle under the GDPR, and to ensure data protection by design and by default. Data controllers are also required to implement safeguards to protect the rights of data subjects pursuant to Article 25(1) GDPR, to ensure data protection by design.

124. It is not within the remit of the DPC, or the scope of the GDPR, to make binding legal determinations on whether a controller has created a safe online platform for Child Users. Nevertheless, consideration of the measures and safeguards adopted by TTL in connection with Articles 24 and 25 GDPR are relevant issues for determination, which are addressed in this Decision.

125. The Statement of Issues sets out the relevant features relating to the platform settings that fall to be examined with regard to Articles 5, 24 and 25 GDPR.

126. All new TikTok accounts, including Child User accounts, were set to public by default. Child Users were presented with a pop-up notification inviting them to 'Go Private' or to 'Skip'. This notification stated that, with a private account, only approved followers could view their content on TikTok and that public accounts were viewable by anyone.[57] It further stated that the user could change their preferences in the app settings at any time.[58]

127. The implications of a private account were explained below the selection button in the app's settings on the 'Privacy' page. When seeking to change from a private to public account, a pop-up notification stated the implications of doing so and invited the user to 'cancel' or 'confirm' this selection. There was no such pop-up when changing from a public to private account.[59]

---

[56] Submissions dated 14 April 2022 at [23]-[25].

[57] Per the Response to the PDD at Footnote 12, TTL states that "*the notification in question (Image 1 of the October 2021 Response, April 2022 Response and this Response) explains that videos and not accounts were viewable by anyone: 'With a private account, only approved followers can view your content on TikTok. Otherwise, your videos can be viewed by anyone'.*"

[58] Response to the Notice of Commencement at [10.2]-[10.3] and Image 1 and 2.

[59] Response to the Notice of Commencement at [10.4]-[10.5] and Image 3.

128. When such public account users, including Child Users, posted a video, such videos were published publicly by default ('Everyone').[60] When doing so, users could further restrict the individual video to 'Friends' (those who followed the user and who the user followed back) or 'Private' (only the user themselves).[61] The user could also determine if the video could be commented upon and interacted with by 'Duet' (which allows users to post a video side-by-side with another user's video) or 'Stitch' (which allows users to combine the user's video with another on the platform). All were enabled by default.[62]

129. When public account users sought to publish a public video, a pop-up notification explained the implications of doing so, asking the user to 'cancel' or 'Post Now'. The 'cancel' button gradient colour was a light grey and the 'Post Now' was black.[63]

130. When posting a video, private account users could select between 'Followers' (those who followed the user and had been approved by the user to do so), 'Friends', and 'Private' or 'Only Me'. A private account user could also choose to disable or enable comments, which were enabled by default. Private account users' videos could not enable 'Duet' or 'Stitch'.[64] Both public and private account users could revisit the above settings on individual videos at any time.[65]

131. Public account users could allow 'Everyone', 'Friends' or 'No One' to comment on individual videos. Private account users could allow 'Followers', 'Friends' or 'No One' to comment. Comments were enabled by default for users who opted for a public account, and set to the same privacy level ('Everyone', 'Followers', etc.) as the video had been.[66] As well as these account-level settings, there were also video-level settings, which allowed users to toggle enable/disable comments on a particular video. If enabled, this would follow the account-level setting.[67]

132. Public account users could determine who could 'Duet' and 'Stitch' their individual videos – 'Everyone', 'Friends' and 'Only Me'. 'Duet' and 'Stitch' were allowed by default for public account users, and set to the same privacy level as the video had been.[68] These were account-level settings and not individual video-level settings and there were also video-level controls that could, either at the time of posting or at any time afterwards, enable or disable 'Duet' and 'Stitch'. Where a user chose 'No One'/'Only Me' at account-level, the 'Duet' and 'Stitch' features were disabled for videos, and could not be enabled through the video-level settings.[69]

---

[60] Response to the Notice of Commencement at [10.9].

[61] Per Response dated 21 February 2022 at 3 and footnote 3, both 'Private' and 'Only Me' meant that only the user who posted the relevant content could view or engage with it, but no other user could. In terms of the audience setting for videos, the term 'Private' was used during the period from 29 July 2020 to 31 December 2020. The terms 'Only Me' and 'No One' were interchangeably used for the 'Duet' and 'Stitch' functions. These terms changed between versions of the platform but the effect remained the same.

[62] Response to the Notice of Commencement at [10.8], Images 4 and 5, and Footnotes 12-17.

[63] Response to the Notice of Commencement at [10.9] and Image 6.

[64] Response to the Notice of Commencement at [10.10].

[65] Response to the Notice of Commencement at [10.11].

[66] Response to the Notice of Commencement at [10.12] and Images 7 and 8, and Response dated 21 February 2022 at 3 and 5.

[67] Submissions dated 14 April 2022 at [34].

[68] Response to the Notice of Commencement at [10.13] and Images 8 and 9, and Response dated 21 February 2022 at 5 and 6.

[69] Submissions dated 14 April 2022 at [34].

133. Private and public account user privacy preferences applied prospectively and could be changed by the user.[70]

134. Public account users could control if other users could download their videos. Private account users' videos could not be downloaded. The download of public account users' videos was disabled by default for under-16 users. Prior to 25 October 2020, for under-16 users the download setting of videos was set to 'off' but could be turned 'on'. From 25 October 2020, TTL enabled restrictions which precluded the download of under-16 users' videos entirely. From January 2021, the download setting was set to 'off' for users aged 16-17.[71] TTL disabled downloads for new and existing under-16 users in Ireland, Italy, and the Netherlands in October 2020. In January 2021, TTL disabled downloads for new and existing users in the remaining EU countries where that feature was in operation.[72]

135. Users could block other users. This blocked all engagement from the blocked user, whether by comments, direct messages, follows or likes.[73]

136. From October 2020, Child Users only received account recommendations for other Child Users and their accounts were not recommended to users aged above 18.[74]

137. TikTok also had a 'Family Pairing' setting. This allowed a Child User to link their account to a non-Child User's account. The linking process involved the generation by the non-Child User of a QR code on the platform, which was then scanned by the Child User who then confirmed if they wished for the accounts to be linked.[75]

138. The non-Child User could manage the Child User's screen time, turn on restricted mode for restricted content, turn on and off access to the search bar, turn on and off the ability to send direct messages (if over 16 years). From November 2020, the non-Child User could choose if the Child User's account was public or private, who could see the Child User's liked videos, limit who could comment on videos generally, and choose if the Child User's account could be suggested to other Child Users.[76] The non-Child User could not monitor the Child User's activity or movements. The Child User could see, via a dashboard, the choices made by the non-Child User. The Child User could disable 'Family Pairing' at any time, which notified the non-Child User. There was no verification of the non-Child User's relationship to the Child User.[77]

139. Users under 16 could not 'Live Stream'. Users under the age of 18 were not permitted to purchase or receive virtual items, which included virtual coins that may be purchased and exchanged for virtual gifts.[78]

---

[70] Response to the Notice of Commencement at [10.14].
[71] Response to the Notice of Commencement at [10.19] and Images 12 and 13, and Response dated 21 February 2022 at 7. This initially referred to being in effect from 25 October 2020, per Footnote 197 of the Response to the PDD, this was clarified as being from January 2021 in fact.
[72] Submissions dated 14 April 2022 at [34].
[73] Response to the Notice of Commencement at [10.20] and Image 14.
[74] Response dated 21 February 2022 at 8.
[75] Response dated 21 February 2022 at 8.
[76] Response dated 21 February 2022 at 8.
[77] Response to the Notice of Commencement at [10.26]-[10.28], and Response dated 21 February 2022 at 9.
[78] Response to the Notice of Commencement at [12.2.8]-[12.2.9].

140. For the sake of completeness, as set out in its Submissions dated 14 April 2022, both during and following the Relevant Period, TTL has implemented a number of changes to its platform settings in relation to Child Users:

> *Private Accounts*
> *(A) From January 2021, under 16 Users were no longer required to make the choice during the account registration process to choose a private account or skip the private account option. Instead, these younger Users' accounts are defaulted to private, without any ability for these younger Users to choose a public account during the registration process. These younger Users are informed through a pop-up notification during the registration process that their account has been set to private (so that only approved Users can view their videos) and that they can review and manage their account through their app settings.*
>
> *Duets and Stitches*
> *(B) From January 2021, the Duet and Stitch feature was disabled for all under 16 Users, meaning that other Users cannot Duet or Stitch with videos created by under 16 Users.61 By default, only "Friends" of Users aged 16 or 17 can make Duets and Stitches of videos created by these Users.*
>
> *Video Comments*
> *(C) From January 2021, under 16 Users do not have the option of allowing their videos to be commented on by "Everyone" and can only choose to receive comments from "Friends" or "No One".*
>
> *Downloading Videos*
> *(D) From January 2021, for younger Users aged 16 or 17, the download feature was turned "off" by default.*
>
> *Suggest Your Account to Others*
> *(E) From January 2021, this setting is turned off for under 16 Users by default.*[79]

141. For the purposes of this Inquiry, I note TTL's contention that its processing prior to these changes was compliant with the GDPR.[80] The subsequent changes do not fall within the scope of this Inquiry, and I assume that these changes are without prejudice to TTL's prior contention that it has, at all material times, complied with the GDPR, including prior to the recent changes and during the periods considered by this Inquiry.

142. As per the Statement of Issues, the first matter for determination is whether, having regard to the default public settings applied to Child Users' accounts, TTL implemented appropriate technical and organisational measures pursuant to Article 24 GDPR to ensure and to be able to demonstrate that its processing of Child Users' personal data was performed in accordance with the GDPR.

143. In this regard, TTL states that 'privacy-friendly account registration process', a series of user controls and just-in-time notifications that implement data protection by design, as well as parental controls and measures to remind Child Users of their settings before posting their videos were in place during the Relevant Period, were informed by a careful review of the

[79] Submissions dated 14 April 2022 at [76].
[80] For example, Submissions dated 14 April 2022 at [76].

relevant privacy risks, as documented in the various data protection impact assessments; and were appropriate measures, having regard to the obligations under Article 24 GDPR.

144. The second matter for determination is whether, having regard to the default public settings applied to Child Users' accounts, TTL complied with its obligations under Article 5(1)(c) and 25(1) GDPR to ensure that its processing of Child Users' personal data was adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed; and to implement appropriate technical and organisational measures designed to implement the data minimisation principle in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

145. In this regard, TTL states that the measures and default settings in place during the Relevant Period were appropriate and complied with its obligations under *inter alia* Articles 5(1)(c), 25(1) (with regard to Article 5(1)(c)), and 25(2) GDPR in light of:

    (a) the purpose of the platform and related context of the processing which would have informed Child Users' expectations;

    (b) the account registration process which, in particular, required Child Users to intervene and make a choice, before the account could be used, as to whether to make their account private or to skip the private account option;

    (c) the suite of privacy controls provided to all users, including Child Users;

    (d) the presentation of a user's video-level settings to the user before they posted a video (each time they posted a video);

    (e) the backend protections on the platform; and

    (f) the transparency information provided to Child Users.

146. The third matter for determination is whether, having regard to the default public settings applied to Child Users' accounts, TTL complied with its obligation under Article 25(2) GDPR to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed.

147. In this regard, TTL also states, as above, that the measures and default settings in place during the Relevant Period were appropriate and complied with its obligations under *inter alia* Articles 5(1)(c), 25(1) (with regard to Article 5(1)(c)), and 25(2) GDPR in light of:

    (a) the purpose of the platform and related context of the processing which would have informed Child Users' expectations;

    (b) the account registration process which, in particular, required Child Users to intervene and make a choice, before the account could be used, as to whether to make their account private or to skip the private account option;

    (c) the suite of privacy controls provided to all users, including Child Users;

(d) the presentation of a user's video-level settings to the user before they posted a video (each time they posted a video);

(e) the backend protections on the platform; and

(f) the transparency information provided to Child Users.

148. The fourth, and final, matter for determination is whether, in circumstances where the platform settings allowed an unverified non-Child User to access and control a Child User's platform settings, TTL complied with its obligations under Articles 5(1)(f) and 25(1) GDPR to ensure that its processing of Child Users' personal data was carried out in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and to implement appropriate technical and organisational measures designed to implement the integrity and confidentiality principle in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

149. In this regard, TTL states that the 'Family Pairing' feature was a useful tool to ensure the safety of Child Users, which did not provide the non-Child User with a way to access the content of the Child Users' messages or their videos, nor did it allow guardians to select privacy settings which were less privacy-friendly than those chosen by the Child User. In these circumstances, TTL states that it is satisfied that it complied with its obligation under Article 5(1)(f) GDPR to process personal data in connection with the 'Family Pairing' feature in a manner that ensured appropriate security of the personal data, and with its obligation under Article 25(1) GDPR in respect of the integrity and confidentiality data protection principle.

150. In the Response to the PDD, TTL made further submissions. Primarily, TTL stated that there was no public-by-default processing. This submission has been considered in full and, for the reasons already set out earlier in this Decision, I do not accept this.

151. Additionally, in relation to Article 25(1) GDPR, TTL states:

> *The fact that a User's video could be seen by a wider audience if published publicly had no bearing on the quantity or quality of the personal data collected by TikTok or the question as to whether the processing operations undertaken by TikTok were necessary for the purpose for which the personal data was processed, i.e. posting a User's video on the Platform. Consequently, Article 5(1)(c) is not apposite in this context.*
>
> *Without prejudice to the foregoing, insofar as Article 5(1)(c) GDPR is interpreted as restricting the manner in which personal data is processed, and therefore deemed applicable to the processing of younger Users' personal data made available via public accounts, TikTok still complied with the data minimisation principle. TikTok acted in accordance with the relevant younger User's settings (e.g. that the videos could be viewable by anyone). Videos were only made public where necessary to give effect to a younger User's chosen settings and, consequently, TikTok did not engage in unnecessary processing by doing so. Indeed, a finding to this effect would not be consistent with the principle of data subject autonomy as protected by Article 8 of the EU Charter of Fundamental Rights.*[81]

[81] Response to the PDD at [5.9]-[5.10].

And:

> *The PDD, in finding that the measures in place were not appropriate, does not properly have regard to:*
>
> > *(A) TikTok's account choice design, which was not public-by-default and, instead, required new Users to elect to opt for either a public or private account;*
> > *(B) the required engagement with User controls before posting;*
> > *(C) the backend protections and available features on the Platform that limited the accessibility of videos, including: (i) the exclusion of videos of younger Users under 16 from the For You Feed; (ii) dispersion of videos of younger Users aged 16-17 in the For You Feed; and (iii) limited search functionality;*
> > *(D) key aspects of how the comments features worked and the safeguards in place, such as the fact that unregistered Users could not use the comments feature and comments by registered Users were moderated for potential harmful content;*
> > *(E) key aspects of how the Duet and Stitch features worked; and*
> > *(F) the transparency information provided to younger Users.*[82]

152. As well as this, TTL states that issues within the scope of this Inquiry have been expanded by the PDD beyond Article 5(1)(c), to include other aspects of Article 5(1). TTL also makes further submissions with regard to Article 25(2).[83]

153. In relation to Article 24 GDPR, TTL states that:

> *Preliminary Finding #2 is based on the DPC's provisional conclusion that TikTok's processing of the personal data of younger Users results in risks to younger Users because of the possibility that dangerous individuals may contact them via comments or otherwise use the data that younger Users make publicly available* [...] *As explained in section 4 above, TikTok disagrees with this conclusion. The DPC's assessment has not properly taken into account the safeguards and measures in place which mitigated the risk of unwanted communication between younger Users and third parties. In addition, the risks in question are those which are associated with younger Users on the Internet, which are distinct from GDPR compliance (as acknowledged by the PDD at paragraph 114).*
>
> [...]
>
> *With respect to the concerns raised in section 5.112(A) above, it is firstly important to appreciate that unregistered TikTok website Users did not have the ability to comment on content. This fundamental point was not appreciated by the DPC, as evident from the above quote.*
>
> [...]

[82] Response to the PDD at [5.30]. See also [5.32]-[5.60].
[83] Response to the PDD at [5.80]-[5.104].

Furthermore, the DPC's assessment fails to properly take into account the back-end protections and available features on the Platform that limited the accessibility of younger Users' videos, and in turn the ability to comment on them, such as the (i) exclusion of videos of younger Users under 16 from the For You Feed; (ii) dispersion of videos of younger Users aged 16 - 17 in the For You Feed; and (iii) limited visibility of younger Users in search

[...]

With respect to the concerns raised in section 5.112(B), no content was made automatically publicly available. Content was made public after at least two interventions by the younger User. The disclosures made and information provided ensured that younger Users made an informed decision before sharing their video content publicly. In particular, the Account Information Pop-Up clearly explained that younger Users could change their account type in the app settings at any time so that their videos would not be made public. Younger Users could also control who could view and comment on their videos for a particular video in the intuitive video settings that were presented to Users as part of the video creation process and before they proactively posted the video.

[...]

The suggestion that younger Users would lack the technical knowledge to know how to change their settings is not supported by any evidence and is inconsistent with findings. For example, an Australian eSafety Commissioner Report which surveyed over 3000 users aged 8-17, found that 68% of young people who use online services in Australia had tried to actively manage their online privacy within the past 12 months, with 43% having increased their privacy settings. These findings suggest that younger Users understood how to use the choices provided to them and could exert control on what they want to share, and with whom.[84]

154. With regard to the 'Family Pairing' platform setting, TTL states:

In short, Younger Users over 16 years old were never exposed to direct messaging from individuals that were not Friends because unknown third parties could not send them a direct message. The DPC's concern that "third parties" could contact the Younger User is therefore not warranted on the facts. Consequently, even during the limited period when direct messaging could be turned on by a guardian for younger Users aged 16 - 17, there was no breach of Article 5(1)(f) GDPR, and the measures in place were appropriate to effectively implement the integrity and confidentiality principle and to protect younger User's rights.

[...]

From mid-November 2020 onwards, guardians could only make the privacy settings of younger Users stricter through Family Pairing. In other words, they could only disable the direct message function entirely in the event that the younger User aged 16 or 17 had previously chosen to enable direct messaging with their Friends.

[...]

[84] Response to the PDD at [5.110]-[5.117].

However, the PDD does not properly take into account the steps required to enable Family Pairing in the first instance and TikTok submits that the PDD is based on a misunderstanding of the position. As previously described in section 3.2.2 of the April 2022 Response and as summarised below, guardians were and are verified for the Family Pairing function. [...]

[...]

These verification steps made it highly unlikely that a non-guardian could pair their account with a younger User, mainly because: (a) the relevant person needed to be physically proximate to the younger User for the younger User to scan the QR code on the younger User's device (meaning the non-guardian would have been known to the younger User); and (b) the 2-Step Confirmation process required the younger User to have twice accepted that they wanted to Family Pair their TikTok account with the person. The younger User, at all times, had access to a dashboard where they could see the choices made by their guardian which ensured complete transparency as to the choices the guardian made for them. Further, the younger User had the option to disable Family Pairing at any time, should they have chosen to do so.

[...]

The ability for a Friend to message a younger User, had a guardian enabled this, did not lessen the security of the relevant younger User's data, nor have any other impact on their data. It is difficult to see how or why the integrity and confidentiality principle is engaged in these circumstances. Simply put, the receipt of a message, in and of itself, is not the "unauthorised or unlawful processing" of the recipient's personal data, nor does it comprise the "accidental loss, destruction or damage" of such data. A younger User could of course have chosen to reply to a Friend's direct message, but this was a decision they were free to make, maintaining the control the younger User had over their data and the confidentiality of this data. Where the younger User replied to the message from a Friend, the recipient of the message was reasonably authorised to read any of the sender's personal data that the sender chose to include in that message.[85]

155. As already noted above, TTL submitted the Marwick Report on 7 September 2022. Prof. Marwick states that she is an associate professor in the Department of Communication and principal researcher at the Center for Information, Technology, and Public Life at the University of North Carolina at Chapel Hill. She conducts qualitative social science research on the social, cultural, and political impact of social media and her areas of expertise include online privacy and surveillance; social practices on social media; and disinformation on social media[86].

156. The Marwick Report was accompanied by a cover letter which submitted that the DPC should revise Findings 1 and 5 of the PDD in light thereof. As set out in both the cover letter and the report itself, Prof. Marwick examines two discrete questions:

    i. *Would a younger User understand the content of the Account Information Pop-Up and the First Post Pop-Up?*

[85] Response to the PDD at [5.131]-[5.141].
[86] The Marwick Report at [1] and Appendix A

ii. *Would a younger User, when joining TikTok or posting a video, understand the terms "public," "anyone," or "everyone," and the significance and consequences of those terms, including that information posted publicly will be widely accessible online - having regard to both their background knowledge and the plain meaning of those terms?* [87]

157. I have considered both the cover letter of 7 September 2022 and the Marwick Report in this regard.

Analysis

158. In relation to the public-by-default account settings, in light of the risks already outlined above which are of high severity, it is unclear why TTL allowed the accounts of Child Users to be set to public-by-default. While, during the registration process the Child User was prompted to select between 'Go Private' and remaining public, the Child User could opt to simply 'skip' this. This use of language would seem to incentivise or even trivialise the decision to opt for a private account. A public account was viewable not only by every single TikTok platform user via the app and every single TikTok platform user via the website, but also by an effectively unlimited number of persons who were not registered TikTok users on the website. The implications of this are particularly severe and wide-ranging – the content published by a Child User on the TikTok platform where the account was public-by-default and not otherwise restricted by individual video-settings could be accessed, viewed and otherwise processed beyond the control of the data subject and TTL.

159. As well as having implications for the publicly viewable account in itself, the public-by-default account then had a series of cascading implications for other platform settings for the Child User.

160. First, this setting meant that a Child User's public account would allow videos to be posted publicly by default too. While TTL notes that there are indeed granular level settings for each individual video and that, when a video was to be posted publicly for the first time,[88] a Child User would be 'nudged' to select between 'Post Now' and 'Cancel', plainly the platform settings incentivized the selection of the posting of videos publicly, given both the phraseology used and the difference in colour gradient. As noted above, where a video was posted publicly on a public account, this had the effect of being viewable and accessible by an unlimited audience.

161. Second, the decision for a Child User's account to be public-by-default also meant that comments were also enabled publicly-by-default. This meant that any registered TikTok user, whether adult or child, could comment on the video of a Child User and interact with them via these comments. The potential for abuse of this platform setting by bad actors is again open-ended as persons could utilise this feature to contact Child Users directly. While comments are, of course, not comparable to direct messages – where users can privately message each other – the potential for ill consequences remains.

162. Third, a public-by-default account also meant that the 'Duet' and 'Stitch' features were also enabled by default. This meant that these features – which allow users to post a video side-by-side with another user's video or which allows users to combine the user's video with another

[87] TTL, Correspondence of 7 September at [1.4] and the Marwick Report at [10].
[88] See Response to the PDD at [5.41].

on the platform, respectively – provided a means for any other users to utilise a Child User's video content.

163. Further to this too are my findings, set out in detail below, in relation to the information available to Child Users, both at the time of registration for a TikTok account and subsequent to it, in relation to the extent to which their personal data would be made available to other registered TikTok users and, more importantly, to the world-at-large. As set out below, the lack of transparency, both in itself and in relation to the use, or rather lack of use, of information relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language, adds to the lack of appropriate technical and organisational measures employed by TTL with regard to its platform settings and Child Users.

164. I do not accept TTL's contention that the technical and organisational measures identified were appropriate to mitigate the risks identified. While TTL asserts that a range of tools to both preemptively alert Child Users to the implications of a public account and a number of specific backend protections relating to the downloading of videos, the suggesting of accounts of Child Users to other accounts and the precluding of under 16s from using certain settings such as 'Live Stream', were appropriate, the measures identified do not address the risks that arise by virtue of the public-by-default account setting at all, and rather act to mitigate the risks from those discrete platform settings themselves.

165. I also do not accept TTL's contention that, having regard to the purpose of the platform and related context of the processing which would have informed Child Users' expectations, this in any way ameliorates the risks to Child Users, or how, in the circumstances, a Child User's experience or expectations would have been disproportionately or adversely affected by private-by-default settings, such as those that TTL has implemented since the Relevant Period. This is particularly the case given that any other registered TikTok user could view the account and videos of a Child User with a public account, as well as Duet and Stitch their videos, and interact with the Child User via comments, and where any person whatsoever could view the Child User's account or videos via the website, regardless of whether or not they were registered and, thereafter, utilise and process the personal data therein in a manner beyond the control of the data subject and TTL.

166. TTL notes there were approximately an average of [redacted] registered EU Child Users during the Relevant Period, a significant cohort of users who were defaulted to a public account. I am, accordingly, of the view that TTL's practice of doing so had the direct result that the processing of personal data of Child Users was not adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and was not appropriate for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

167. Further, the processing at issue, whereby public-by-default account settings applied, makes the social media content of Child Users visible to anyone on or off the TikTok platform. This increased visibility of Child Users poses a severe possible risk that dangerous individuals may seek to communicate directly with Child Users.

168. I do not agree that TTL acted in accordance with the relevant Child User's settings to give effect to a Child User's chosen settings and, consequently, TTL did not engage in unnecessary processing by doing so and that such a finding to this effect would not be consistent with the principle of data subject autonomy, as protected by Article 8 of the EU Charter of Fundamental Rights. I have had full regard to all submissions made by TTL during the Inquiry in this regard,

including TTL's submissions that the settings were designed to safeguard Child Users, to provide them with the benefits of the relevant features, and how those features were important to the core purpose of TikTok. As set out above, the further implications of the public-by-default processing meant that indeed this was not a choice made by Child Users.

169. Finally, I also do not agree that the PDD in any way expands upon the scope of the Inquiry. TTL seems to premise this entirely on the basis that paragraph 86 of the PDD referred to "Article 5" rather than Article 5(1)(c) GDPR, and that this had the effect of bringing the principles of purpose limitation and integrity and confidentiality into scope.[89] This is not the case and I am happy to make this clear.

170. Having considered the Marwick Report in full, it is unexplained, in either the cover letter or the report itself, exactly how the contents of the report – that is the analysis of the young person's understanding of terminology and the implications of privacy settings, as well as Prof. Marwick's evidence in those regards – disturbs the substantive findings in the PDD regarding the public-by-default processing of the relevant features. While Prof. Marwick provides detailed analysis in relation to the issues regarding transparency, considered in detail below, at no point does she make any submissions regarding the substantive conclusions in the PDD in relation to the fact of public-by-default processing. The cover letter of 7 September 2022 similarly makes no substantive submissions in this regard, aside from twice asserting that Finding 1 should be revised. On this basis, having considered the report, for the reasons set out below, I reject the report's conclusion that the platform settings and relevant features were sufficiently transparent.

171. Having considered the measures and safeguards implemented by TTL in respect of this, I am of the view that these measures and safeguards do not properly take into account the specific risks to the rights and freedoms of Child Users which are at issue, as set out above. In particular, where a Child User chose to 'skip' opting for a private account, this had the cascading effect of allowing many further platform settings be rendered public – including the accessibility of comments on video content created by the Child User. I also note, in the context of Article 25(1) GDPR, that this processing does not comply with the principles of data minimisation and data protection by default, as set out above.

172. Having considered the risks posed, I am of the view that the measures and safeguards that were implemented by TTL failed to implement the requirements of the GDPR or to protect the rights of Child Users, as required under Article 25(1) GDPR, as, 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, TTL did not, 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 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 the GDPR and protect the rights of data subjects.

Finding 1

At the time of the Relevant Period, TTL implemented a default account setting for Child Users which allowed anyone (on or off TikTok) to view social media content posted by Child Users. In this regard, I am of the view that TTL failed to implement appropriate technical and

[89] Response to the PDD at [5.61]-[5.79].

organisational measures to ensure that, by default, only personal data which were necessary for TTL's purpose of processing were processed.

In particular, this processing was performed to a global extent and in circumstances where TTL did not implement measures to ensure that, by default, the social media content of Child Users was not made accessible (without the user's intervention) to an indefinite number of natural persons. I am therefore of the view that the above processing by TTL was contrary to the principle of data protection by design and default under Article 25(1) and 25(2) GDPR, and contrary to the data minimisation principle under Article 5(1)(c) GDPR.

173. For the purposes of assessing TTL's compliance with Article 24 GDPR in relation to the public-by-default setting, I have considered the nature, scope, context and purpose of the processing which results from this setting. Having considered these four factors, I have concluded that the processing of the personal data of Child Users results in a severe possible risk to the rights and freedoms of Child Users, to the extent that dangerous individuals may avail of the public-by-default setting to contact Child Users via comments and utilise and process the personal data of Child Users on their public-by-default accounts.

174. I do not accept TTL's submission that my assessment has not properly taken into account the safeguards and measures and backend protections in place which mitigated the risk of unwanted communication between Child Users and third parties, nor do I accept that the risks are somehow inherent to Child Users on the internet more generally, nor have I failed to appreciate that unregistered TikTok website users did not have the ability to comment on content. For the reasons set out in detail above, accounts were, by default, public and viewable by non-registered persons. It is simply not sustainable to state that the platform settings that were implemented were inherent to all Child Users generally on the internet.

175. Further, TTL has specifically referred to the 2018 report by the Australian eSafety Commissioner, which states that 43% of children in the study increased their privacy settings over the preceding 12 months. Leaving aside that the study is pre-GDPR and concerns a non-EU country, it cannot be inferred, as TTL contends, that children made informed choices, in a vacuum, to adjust their privacy settings. The other options contained in the question - "reported someone to my school/parents" "blocked someone", "deleted comments" etc. - suggest that children are reacting to an online harm experienced on social media, rather than making a change on foot of transparency information provided by the controller. The report does not support what TTL has suggested and, indeed, the CNIL study referenced above[90] shows that not all children are aware of the existence of privacy settings and that children have a preference for private accounts by default.

176. TTL has outlined the risk-based measures it has implemented for the purpose of ensuring and demonstrating its compliance with the GDPR with regard to this processing. I have considered these. While I accept that TTL provides certain information, tools and safeguards to users, which promote safety and prevent bad actors from interacting with Child Users, I am of the view that these limited measures were not effective in circumstances where Child Users could be contacted via public comments and where there was little that could be done to safeguard against non-registered users utilising the website. I am therefore of the view that TTL has not properly taken into account the risks posed to the rights and freedoms of Child Users when

[90] Commission Nationale de l'Informatique et des Libertés, 'Les comportements digitaux des enfants' (February 2020) at 24, accessible via https://www.cnil.fr/sites/default/files/atoms/files/sondage_ifop_-_comportements_digitaux_des_enfants_-_fevrier_2020.pdf

implementing measures to ensure its compliance with the GDPR. I further note that, by implementing a public-by-default setting and, therefore, expecting all Child Users as young as 13 years old to have sufficient technical knowledge to change this setting, TTL has created conditions in which unnecessary publication of Child Users' social media content may occur (i.e. more extensive processing of social media content than was intended by the user).

Finding 2

During the Relevant Period, TTL implemented a default account setting for Child Users which allowed anyone (on or off TikTok) to view social media content posted by Child Users. The above processing posed severe possible risks to the rights and freedoms of Child Users.

In circumstances where TTL did not properly take into account the risks posed by the above processing, I am of the view that TTL did not implement appropriate technical and organisational measures to ensure that the above processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR.

177. In relation to the 'Family Pairing' platform setting, TTL asserts that it is a 'privacy-optimising-only feature', while maintaining the Child User's individual autonomy.[91] This platform setting functioned by two TikTok account holders navigating the 'Family Pairing' section and one user – intended to be the Child User – scanning a QR code generated by the other user – intended to be the parent or guardian user. The intended-Child User could disable this at any time, which notified the other user. The intended-Parent/Guardian user could then control the following:

(a) Manage screen time;
(b) Add more stringent restrictions on available content;
(c) Disable access to the search feature;
(d) Enable or disable direct messages for users over 16.

178. From November 2020, further functionality was added, as follows:

(a) Make the account private if public;
(b) Choose if the other users could view 'Liked Videos';
(c) Limit comments;
(d) Chose if the account could be suggested to Child Users.

179. Two discreet issues arise with regard to this platform setting. First, the 'Family Pairing' setting allowed an unverified non-Child User (the intended-Parent/Guardian user) to access and control a(n) (intended) Child User's platform settings. As set out above, any other user could pair their account to that of a Child User and it was not limited to anyone who was a parent or guardian of the Child User. TTL set out that this platform setting did not enable the intended-Parent/Guardian user to see or access the Child User's messages or video content. The intended-Child User could disable the pairing when they wished, although the other user would be notified. Second, and relatedly, the 'Family Pairing' setting generally allows the intended-Parent/Guardian user to apply stricter privacy settings to the intended-Child User's account – narrowing the available content, disabling search and direct messages, making the account private, and limiting comments. However, it also allowed the intended-Parent/Guardian user to make certain features less strict – in particular, enabling direct messages for over 16 year olds.

[91] Submissions dated 14 April 2022 at [49].

180. In those circumstances, if an intended-Parent/Guardian user enabled direct messages, this would result in TTL performing processing operations on the Child User's personal data that enables third parties to contact the Child User via direct messages, which would constitute unauthorised processing of the Child User's personal data. The Child User did not choose to have their personal data used in a manner that enables such contact and it is not clear at all why the intended-Parent/Guardian should be able to choose to enable direct messages and allow the Child User less strict privacy settings than what they themselves have chosen. This particular platform setting stands in contrast to the other platform settings for 'Family Pairing' which allow only for stricter privacy settings.

181. I do not accept that I have not properly taken into consideration the steps for enabling the 'Family Pairing' platform setting. Indeed, TTL's submissions confirm the above reasoning and what is set out above and that none of these steps verify the relationship between the parties, that TTL's referral to the non-Child User as a 'guardian' is aspirational, that TTL has provided no evidence to suggest that it is "highly unlikely" that a "non-guardian" could pair their account with a Child User[92] and, most centrally, that a Child User could have their settings made less private without their input.

182. While generally the control that was vested in the intended-Child User and that the platform settings related to 'Family Pairing' allow the intended-Parent/Guardian user to make the privacy settings stricter, and that the intended-Child User generally retained privacy and control over their personal data in the form of messages and videos, allowing the non-Child User's privacy settings to be loosened in this manner does not ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and is not an appropriate technical and organisational measure designed to implement the integrity and confidentiality principle in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects, per Article 5(1)(f) and 25(1) GDPR. Accordingly, I find an infringement of the GDPR with regard to this aspect of the 'Family Pairing' setting.

Finding 3

During the Relevant Period, TTL implemented a platform setting - called 'Family Pairing' for Child Users whereby a non-Child User could pair their account to that of the Child User. This platform setting allowed the non-Child User to enable direct messages for Child Users above the age of 16. The above processing posed severe possible risks to the rights and freedoms of Child Users.

In circumstances where this processing does not ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and TTL failed to implement appropriate technical and organisational measures designed to implement the integrity and confidentiality principle in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects, I am of the view that this processing was not performed in accordance with the GDPR, contrary to Article 5(1)(f) and Article 25(1) GDPR.

[92] Response to the PDD at [5.136].

G. ISSUE 2: ASSESSMENT AND CONSIDERATION OF MATTERS CONCERNING AGE VERIFICATION PURSUANT TO ARTICLES 24 AND 25 GDPR

G.1 Application of Articles 24 and 25 GDPR

183. The relevant provisions in relation to Articles 24 and 25 GDPR are set out above.

184. TTL has made various submissions regarding Articles 24 and 25 GDPR, above. In relation to the application of these provisions in the context of age verification, TTL further submits:

> *Articles 24(1), 25(1), and 25(2) GDPR are all focused on taking a risk-based approach to data protection compliance. When assessing the risks in the present case, TikTok was aware of the need to strike the balance between: (i) the issues that arise with under-age Users potentially accessing the Service; and (ii) the need to respect data protection rights by taking an appropriate and proportionate approach to user age verification. The approach to user age verification cannot be disproportionate or involve the processing of excessive information since such an approach would, in itself, breach the GDPR, including Articles 24 and 25. During the Relevant Period, TikTok considered technical measures, including the potential use of [redacted]. Having considered and assessed the potential risks identified above TikTok deployed an age verification mechanism which was appropriate, proportionate and in line with data protection principles including data minimisation.*
>
> [...]
>
> *Article 24(1) GDPR is not prescriptive as to how controllers should comply with their obligations. Indeed, such a prescriptive approach would be inconsistent with the objective of these provisions, which is to embed privacy compliance practices into the internal practices of organisations in a manner that works for each organisation.*[93]

And:

> *In order to comply with Article 25(1) GDPR, controllers are asked to weigh a multitude of broad and abstract concepts, assess the risks, and then determine "appropriate" measures. Each of these elements is opaque and open to interpretation, and as a result, no two assessments performed in accordance with Article 25 will look the same. Article 25(1) requires "appropriate" measures, which when applied to age verification would mean that a controller is required to implement measures to determine the age of users with an appropriate, rather than absolute level of certainty. Such measures should not be disproportionate. TikTok's age verification measures restricted access to the service by underage individuals while ensuring that the GDPR data protection principles, such as data minimisation, were implemented in an effective and proportionate manner.*[94]

185. Further:

---

[93] Response to the Notice of Commencement at [15.2]-[15.3].
[94] Response to the Notice of Commencement at [15.5].

It is worth underlining that Article 25(1) GDPR, and similarly Article 24(1) GDPR, only require "appropriate" measures which, when applied to age verification, would mean that a controller is required to implement measures to determine the age of users with an appropriate level of certainty (having regard to the various factors set out in Articles 24/25 GDPR), not with an absolute level of certainty. This is further supported by guidance issued by supervisory authorities. For example, the ICO states that the level of certainty for age verification needs to be "appropriate to the risks to the rights and freedoms of children" rather than an absolute threshold. It is also worth noting that there is no legal requirement under the GDPR or Irish law to verify users' age in a specific way.

Regulatory guidance, including the DPC's Fundamentals, does not (and did not during the Relevant Period) explain what an appropriate age verification mechanism would be in this context. As a result, TikTok was required to develop age verification measures in the absence of clear guidance from, or a consensus among, supervisory authorities as to what was appropriate for the Platform.

TikTok's research continues to show that there is a general lack of agreement regarding what constitutes appropriate age verification solutions. There also continues to be a general lack of concrete guidance regarding the processing of children's data under the GDPR, as demonstrated by the fact that various supervisory authorities have recently been conducting public consultations on this topic. The DPC's recent guidance on the processing of children's data acknowledges that "the technological area of age verification mechanisms and tools is still very much in development." Similarly, the results of the CNIL's public consultation on children flagged the necessity of a harmonisation, at the European level, among the tools retained to perform age verification7 In any case, during the Relevant Period, there was no single alternative, workable age verification solution.

Consistent with the current views of European supervisory authorities, TikTok concluded that collection of hard identifiers (e.g., ID card, passport, driving licence) upon registration would be disproportionate in an age verification context having regard to Article 5(1)(c) GDPR. For example, the ICO's AADC states: "we recommend that you avoid giving users no choice but to provide hard identifiers unless the risks inherent in your processing really warrant such an approach. This is because some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults."[95]

186. TTL's submissions have been taken into consideration in full.

G.2 Analysis and findings regarding TTL's compliance with Articles 5, 24 and 25 GDPR in connection with age verification

Overview of Issues and Technical and Organisational Measures

187. The Statement of Issues sets out the relevant features relating to age verification that fall to be examined with regard to Articles 24 and 25 GDPR.

[95] Submissions dated 14 April 2022 at [132]-[135].

188. Users of TikTok should be aged 13 and above.[96] During the period from 29 July 2020 to 31 December 2020, TikTok was rated in the Apple App store as '12+' and in the Google Play store as 'Parental Guidance Recommended'.

189. Individuals who wish to use TikTok must also confirm their date of birth via an age gate. Individuals are asked to insert their date of birth. No indication is provided for why this is necessary nor does the selection default to an age over 13.[97]

190. When individuals insert a date of birth below 13 years of age, the registration process ceases. A pop-up notification states the individual is not eligible for TikTok. Individuals who seek to re-enter a date of birth, whether above or below 13, are shown the same notification, and those who re-install the platform app on their device.[98]

191. Individuals under the age of 13 who entered a date of birth above 13, 16 or 18 years gained access to the age-relevant platform settings indicated above.

192. During the period from 29 July 2020 to 31 December 2020, TTL had a number of measures to remove users under the age of 13 who accessed the platform. If TTL believed a user was under 13, they were removed.[99]

193. From August 2020, users and non-users could report a user under 13 using a webform and via the app.[100] This webform was called 'Request Privacy Information', accessible via the 'TikTok Help Centre' and the 'TikTok Safety Centre' on both the website and the app. Reported accounts were referred to moderators.

194. TTL also used [redacted] to identify if an account was held by a user under 13 where such [redacted][101] Where an account did, it was referred to moderation.

195. If a moderator in another area considered a user was under 13, they could refer the account for moderation or could action removal of the account themselves.[102]

196. Moderation of an account suspected to be operated by a user under 13 involved moderators having regard to data such as the [redacted] Moderators consider factors such as [redacted][103]

---

[96] Response to the Notice of Commencement at [14.1], TikTok, 'TikTok Terms of Service' (July 2020) and TikTok, 'TikTok Privacy Policy' (July 2020) and TTL's under-18s summary of its Privacy Policy.
[97] Response to the Notice of Commencement at [14.3] and Image 19.
[98] Response to the Notice of Commencement at [14.4] and Image 20.
[99] Response to the Notice of Commencement at [14.5].
[100] TikTok, 'Request Privacy Information' accessible via https://www.tiktok.com/legal/report/privacy . Prior to this during the Relevant Period, a privacy alias privacy@tiktok.com was made available to users for reporting purposes via the link https://www.tiktok.com/legal/report/privacy in addition to the app reporting, the Final Submissions at [8.1].
[101] Response to the Notice of Commencement at [14.10] and Submissions dated 14 April 2022 at [137].
[102] Submissions dated 14 April 2022 at [137].
[103] Response dated 21 February 2022 at 9.

197. TikTok does not require the provision of identity verification documentation in the registration process (for example, passport, national identity card, etc.).[104]

198. As already noted above, during the period of 29 July 2020 to 31 December 2020, the approximate total average number of registered EU TikTok Child Users under the age of 18 was [redacted] TTL does not retain data to determine the approximate number of TikTok users that were identified as being under the age of 13 when attempting to register during the period from 29 July 2020 to 31 December 2020; however, TTL believes that the approximate number of individuals in the EU who were failed registration on the basis of their identifying as an individual below 13 years of age during the equivalent number of days from 14 April to 16 September 2021 was [redacted] During the period of 29 July 2020 to 31 December 2020, the approximate number of EU TikTok users that were detected as being under 13 subsequent to their registration and removed from the platform was [redacted]

199. The Statement of Issues identified three matters for determination, in this regard.

200. First, the question of whether, having regard to TTL's requirement that users of TikTok should be aged 13 and above, TTL complied with its obligation under Article 24 GDPR to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that its processing of personal data of Child Users was performed in accordance with the GDPR, including by implementing measures to ensure against children aged under 13s being able to access the platform.

201. In this regard, TTL states that it implemented measures during the Relevant Period which included a combination of measures to prevent children under 13 from using the app and to remove under 13 users if they did manage to register, were effective and appropriate. These included:

    (a) Individuals registering for a TikTok account had to go through an age gate. Individuals were not informed that their date of birth was used for age-gating purposes.

    (b) If a Child User entered a date of birth corresponding to an age under 13 in the app, [redacted]

    (c) This was also implemented for users who signed in via a third-party account (e.g., Google, Facebook).

    (d) TikTok was rated in the Apple App store as "12+" and in the Google Play store as "Parental Guidance Recommended".

    (e) When it was determined that an account had been created by someone who was under 13, the account was closed and deleted. [redacted] A user's account could also be reviewed if it was reported by a parent or anyone else that the reported user was under 13. The Privacy Policy specifically

[104] Response dated 21 February 2022 at 9.

invited individuals to contact TTL, via a linked web form, if they believed it had personal data about a child under 13.

(f) An in-app reporting function could be used by users to report accounts to content moderators, including where they believed such accounts belonged to users who were under 13.

(g) Where under 13 users were removed from the platform, a [redacted]

202. Second, the question of whether, having regard to TTL's requirement that users of TikTok should be aged 13 and above, TTL complied with its obligations under Article 5(1)(b), 5(1)(c) and 25(1) GDPR to ensure that it collected Child Users' personal data for specified, explicit and legitimate purposes and that it did not further process that data in a manner incompatible with those purposes; to ensure that its processing of Child Users' personal data was adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; and to implement appropriate technical and organisational measures designed to implement the purpose limitation and data minimisation principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects, including by implementing measures to ensure against children aged under 13's access to the platform.

203. In this regard, TTL also states that it implemented effective and appropriate measures during the Relevant Period, which included a combination of measures to prevent children under 13 from using the app and to remove under 13 users if they did manage to register.

204. Third, and finally, the question of whether, having regard to TTL's requirement that users of TikTok should be aged 13 and above, TTL complied with its obligation under Article 25(2) GDPR to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed, including by implementing measures to ensure against children aged under 13s being able to access the platform.

205. In this regard, TTL also states that it implemented effective and appropriate measures during the Relevant Period, which included a combination of measures to prevent children under 13 from using the app and to remove under 13 users if they did manage to register.

206. TTL has indicated that, while it believes that the age verification measures that were in place during the Relevant Period complied with the GDPR, it is also currently proposing [redacted] so that appropriate action may be undertaken.[105]

207. In the Response to the PDD, TTL made further submissions regarding age verification, in particular that a finding that implementing a default account setting for Child Users which allowed anyone (on or off TikTok) to view social media content posted by Child Users was contrary to Article 24(1) GDPR, was not compatible with the finding that TTL's age verification measures were compliant and, as such, is not sustainable.[106] As well as that:

[105] Submissions dated 14 April 2022 at [140].
[106] Response to the PDD at [6.10].

While the Children's DPIA may not have expressly referred to the risks to underage children accessing the Platform, these risks were of necessity considered by TikTok when developing the Preventative Measures and Reinforcement Measures. They were the very reason such measures were deployed in the first place.

[...]

TikTok submits that the DPC has erred in the PDD by conflating the question of compliance with Article 24 GDPR with the question as to whether the DPIAs complied with the requirements of Article 35 GDPR, which is an entirely separate question not within the scope of this Inquiry. The DPC has not found that the relevant processing was in breach of the GDPR. Rather, the DPC has found the converse, i.e., that TikTok demonstrated that the age verification measures were appropriate to ensure compliance with the GDPR. It is submitted that, in such circumstances, the DPC cannot find a breach of Article 24(1) GDPR in connection with those measures.[107]

Analysis

208. As previously set out, neither Article 24 nor Article 25 GDPR oblige TTL to implement specific technical and organisational measures, rather, such measures must be appropriate. Accordingly, I agree with TTL's submission that there is no one particular method of ensuring that children under the age of 13 do not access the TikTok platform. Given the findings set out above in relation to the public-by-default processing, whereby the personal data of Child Users was accessible to an indefinite audience and the high risks associated with these platform settings, there is a particular emphasis on TTL to ensure that appropriate standards of data protection measures are in place to safeguard the position of Child Users, both below and above its official user age threshold of 13.

209. TTL has set out numerous measures that it undertakes in order to ensure that children under 13 do not gain access to TikTok and that those who do are removed, the appropriateness of which is examined below. However, during the Relevant Period, in spite of these efforts, approximately [redacted] children were detected as having gained access to the platform and were removed. This constitutes approximately [redacted] of TTL's approximate average number of Child Users during the Relevant Period. The numbers of children under 13 who evaded, and may continue to evade, detection is unclear.

210. Of course, I am conscious that there is no one perfect age verification method or impregnable age gate and it would not be appropriate to determine whether the technical and organisational measures employed by TTL were appropriate through such a lens. Rather, in light of the risks for a child under 13, I must examine if the measure utilised were appropriate.

211. As set out above, while TTL has conducted a data protection impact assessment in relation to Children's Data and Age Appropriate Design, notably this DPIA does not identify the specific risk of children under the age of 13 accessing the TikTok platform and the further risks that may arise from this. While the risks identified in the DPIA apply equally to children under the age of 13 as those over the age of 13, the risks associated with these (under 13) users is exacerbated and particularly severe given their young age and the fact that the TikTok platform is expressly not intended for those under the age of 13. The other data protection impact assessments conducted by TTL similarly do not identify this risk. It is not clear why TTL has not done so. As

[107] Response to the PDD at [6.13]-[6.15].

set out above, TTL has stated that "*these risks were of necessity considered by TikTok when developing the Preventative Measures and Reinforcement Measures*".[108] Aside from baldly stating this, this does not explain how or to what extent such risks were considered.

212. I also do not accept that I have erred "*by conflating the question of compliance with Article 24 GDPR with the question as to whether the DPIAs complied with the requirements of Article 35 GDPR, which is an entirely separate question not within the scope of this Inquiry*".[109] TTL has obligations arising under the GDPR with regard to Article 24 that fall to be determined within the scope of this Inquiry. That TTL did not, in its DPIA, or in the course of this Inquiry, provide evidence that it considered these risks in complying with these obligations is relevant. Article 35 GDPR is indeed not in scope for the Inquiry; however, I reserve the right to determine separately if Article 35 GDPR has been complied with in this regard.

213. Given the implications of children under 13 gaining access to the platform – that is, the public-by-default processing set out above, the type of personal data that such a child could (publicly) share – both the categories of personal data and that such personal data was a child's in itself – the accessibility to this personal data of both other users and non-users via the website, and the potential further processing and/or loss of control over this personal data, TTL should have examined this risk.

214. On this basis, and taking into account that TTL's DPIA failed to identify the specific risk of children under the age of 13 accessing the TikTok platform, I am of the opinion that, TTL did not assess the specific risks to children under 13 gaining access to the TikTok platform. In failing to do so, TTL has therefore failed to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that its processing of personal data of Child Users was performed in accordance with the GDPR, including by implementing measures to ensure against children aged under 13 being able to access the platform.

Finding 4

During the Relevant Period, TTL implemented a default account setting for Child Users which allowed anyone (on or off TikTok) to view social media content posted by Child Users. The above processing posed severe possible risks to the rights and freedoms of Child Users. This also posed several possible risks to the rights and freedoms of children under the age of 13 who gained access to the platform.

In circumstances where TTL did not properly take into account the risks posed by the above processing to children under the age of 13, I am of the view that TTL did not implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the above processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR.

215. As regards the age verification processes that TTL implemented during the Relevant Period, TTL has, as set out above, made extensive efforts to ensure its platform is only accessible to those over the age of 13. This included the implementation of a neutral age gate, [redacted] utilising the age rating of the relevant applications stores in order to avail of age-gating device settings on individual devices, both general and specialist moderation teams to identify those under 13 who had passed through

[108] Response to the PDD at [6.13].
[109] Response to the PDD at [6.15].

the age gate, in- and extra-app reporting functions, and [redacted]

216. As noted above, during the Relevant Period, TTL believes that the approximate number of individuals in the EU who failed registration on the basis of their identifying as an individual below 13 years of age was [redacted], based on an equivalent period, and approximately [redacted] users were detected as being under 13 subsequent to their registration and removed from the platform.

217. I note that TTL did not employ the use of hard identifiers in order to determine the age of children accessing the platform, however, I accept TTL's submission that such a requirement would be disproportionate, given that children, and particularly younger children, are unlikely to hold or have access to such hard identifiers and this would act to excluding or locking out Child Users who would otherwise be able to utilise the platform, as well as that such a requirement would likely disproportionately affect Child Users from minority backgrounds.[110]

218. In examining the technical and organisational measures identified by TTL, I am particularly conscious of the fact that Articles 24 and 25 GDPR do not themselves specify any particular measure that should be utilised in order to ensure age verification or prevent those for whom a platform is not intended to gain access to it. I am conscious too that the area of age verification remains under development and there are yet to be accepted or stipulated industry or regulatory standards in this regard. I am also conscious that there is certainly no absolute method of age verification and that it only falls to me, as decision-maker, to determine if the measures employed were appropriate with regard to 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.

219. Accordingly, on this basis, I proposed, in the PDD and the Draft Decision, to find that the technical and organisational measures in respect of the age verification processes themselves undertaken by TTL during the Relevant Period complied with the GDPR in light of the measures undertaken and the extent to which TTL sought to ensure its platform remained accessible only to those above the age of 13.

G.3 CSA objections and the decision of the EDPB further to the Article 65(1)(a) dispute resolution process

220. Following the circulation of the Draft Decision to the CSAs for the purpose of enabling them to express their views in accordance with Article 60(3) GDPR, the Italian SA raised an objection to the above proposed finding. As it was not possible to reach consensus on the views that were expressed by the Italian SA, this objection was referred to the EDPB for determination pursuant to the Article 65 dispute resolution process. Having considered the merits of the objection, the EDPB determined as follows:

> *166. The EDPB notes that the IT SA's objection, found to be relevant and reasoned in section 5.4.1, requests the IE SA to change the Draft Decision in order to find an*

[110] Response to the Notice of Commencement at [15.7] and Submissions dated 14 April 2022 at [133]-[139].

infringement of Article 25 GDPR insofar it relates to the age verification measures implemented by TTL in the TikTok platform.

167. The EDPB considers that, while the IT SA does not differentiate in its objection between specific parts of Article 25 GDPR, on the basis of its wording and content, the IT SA's objection is targeting specifically an alleged lack of compliance by TTL with Article 25(1) GDPR. Therefore, the scope of the EDPB's analysis in this section covers whether TTL has infringed ***Article 25(1) GDPR ('data protection by design')*** *with regard to the age verification measures implemented by TTL in the context of the TikTok platform during the Relevant Period.*

[...]

175. The EDPB recalls that Article 25(1) GDPR requires controllers to have data protection designed into their processing of personal data and that applies throughout the processing lifecycle. The core of the provision is to ensure appropriate and effective data protection by design, which means that controllers should be able to demonstrate that they have implemented the appropriate measures and safeguards in the processing of personal data to ensure that the requirements of the GDPR are met and that the data protection principles[111] and the rights and freedoms of data subjects are effective[112].

176. As a preliminary remark, the EDPB notes that the measures implemented by TTL (as described in paragraphs 124-125 of this Binding Decision above) constitute of an ex ante part and an ex post part. The ex ante part is comprised of the steps a) - c), whereas the ex post part constitutes f) - i). The points d), e) and j) merely provide additional information about the circumstances of the measures. Further, it must be noted that, while in the context of the Draft Decision the IE SA and TTL refer to 'age verification', indeed, little verification, i.e. the confirmation as true or proofing by good evidence, is taking place[113]. Only one aspect of the ex post measures, the identifying users that in their profile description state to be- below 13, is verifying the age of the user. The remaining measures do not aim at collecting any form of reliable evidence that would allow indeed to verify the age. TTL in this regard acknowledges this by calling its solution under point a) an Age Gate, rather than an age verification process. However, for the sake of consistency, the EDPB will below refer to the ex ante and ex post measures as 'age verification' measures.

177. The EDPB underlines that, in the context of ***Article 25(1) GDPR****, the requirement for the measures to be 'appropriate' means that the measures and necessary safeguards implemented by a controller should be suited to achieve the intended purpose, i.e. they must implement the data protection principles and secure the rights of data subjects 'effectively'[114]. The EDPB notes that the concept of 'effectiveness' in the context of data*

[111] The data protection principles as listed in Art. 5 GDPR.
[112] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 2 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 2.
[113] See definition in Oxford English Dictionary https://www.oed.com/view/Entry/222511?redirectedFrom=verify.
[114] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraphs 7 and 8.

protection law stems from the objective of the GDPR to ensure 'effective protection of personal data throughout the Union'[115].

178. *The EDPB thus disagrees with TTL's assertion that the IT SA seeks to introduce a standard of 'factual effectiveness' rather than 'appropriateness' when assessing TTL's compliance with Article 25 GDPR and that the IT SA's objection incorrectly considers the effectiveness of the age verification measures implemented by TTL*[116].

179. *The EDPB also underlines that, in line with the accountability principle, TTL as the controller is liable to demonstrate its compliance with the data protection principles and its other obligations under GDPR in relation to the processing at stake*[117].

180. *While Article 25(1) GDPR does not require the implementation of any specific technical and organisational measures, and the controller has discretion in respect of the choice of the measures and safeguards, the measures and safeguards chosen by the controller have to be designed to be robust taking into account the risks associated with the processing. The EDPB considers that under Article 25(1) GDPR the requirement of appropriateness is therefore closely related to the requirement of effectiveness*[118]. *Whether or not the measures chosen by the controller in the particular case are appropriate depends on the assessment of the elements listed in Article 25(1) GDPR*[119].

181. *The EDPB therefore proceeds below with an analysis of those elements, in order to assess if the age verification measures implemented by TTL in the present case comply with Article 25(1) GDPR. The analysis will address, in turn: 'nature, scope, context and purpose of processing', 'risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing', the 'state of the art', the 'cost of implementation' and the effectiveness of the measures implemented by TTL in light of the requirements of Article 25(1) GDPR*[120]. *This will be carried out for both the ex ante and the ex post measures implemented by the controller. Finally, based on the elements available to the EDPB in the context of this procedure, the EDPB will assess whether, in accordance with Article 25(1) GDPR, the measures implemented by TTL were appropriate in this particular case.*

'nature, scope, context and purpose of processing'

182. *The EDPB recalls that the concept of* ***nature*** *relates to the inherent characteristics of the processing*[121]. *As stated in the Draft Decision, this case relates to the processing of personal data of children under the age of 13 in the context of the TikTok platform, both*

[115] Recital 11 GDPR. See also CJEU case law, e.g. Judgement of the Court of Justice of 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317, paragraphs 38, 53, 58.
[116] TTL Art. 65 Submissions, paragraphs 6.32-6.33. The EDPB notes that the notion of 'factual effectiveness' is introduced by TTL in its submissions and is not referred to as such in the IT SA's objection.
[117] Art. 5(2) and Art. 24 GDPR, also Recital 74 GDPR.
[118] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 8 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 8.
[119] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraphs 14, 17.
[120] Art. 25(1) GDPR.
[121] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 27 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 28.

mobile application- and website-based, in particular age verification[122]*. As noted in the IT SA's objection, the TikTok platform is a service that is offered directly to children*[123]*.*

183. *The* ***scope*** *refers to the size and range of the processing*[124]*. As described above, TTL does not retain data to determine the approximate number of the TikTok platform users that were identified as being under the age of 13 when attempting to register during the period from 29 July 2020 to 31 December 2020 and therefore provides an assumed approximate number of prevented registrations by users under the age of 13 [redacted]) and an assumed number of accounts of users under the age of 13 being closed proactively by TTL itself ([redacted])*[125]*. The Draft Decision further notes that during the Relevant Period, in spite of the efforts undertaken by TTL, approximately [redacted] of TTL's approximate average Child Users were detected as being under 13, and that the number of children under 13 who evaded, and may continue to evade, detection is unclear*[126]*.*

184. *As noted in the IT SA's objection, the fact that such an amount of profiles was removed means that as many below-13 child users managed to easily access the platform and used it for an unspecified period – not to mention all the below-13 child users of the platform that have remained as yet undetected*[127]*. The Draft Decision also establishes that TTL processed the personal data of at least those children under 13 whose account was detected, and by setting accounts to public by default, TTL ensured that the scope of processing of social media content of those children under 13 was potentially very extensive, being made accessible without restriction to an indeterminate global audience*[128]*.*

185. *As established in the Draft Decision, the accounts of registered TikTok platform users were public-by-default*[129]*. This meant that, for example, a public account was viewable not only by both every single TikTok platform user via the app and every single TikTok platform user via the website, but also by an effectively indeterminate number of persons who were not registered TikTok platform users on the website*[130]*. The implications of this are particularly severe and wide-ranging – the content published by Child Users, including those under the age of 13 who remained undetected, on the TikTok platform where the account was public-by-default and not otherwise restricted by individual video-settings, could be accessed, viewed and otherwise processed beyond the control of the data subject and TTL*[131]*.*

186. *The processing at stake therefore affected a large number of vulnerable persons*[132] *and the extent of the processing of their personal data was potentially very large.*

---

[122] Draft Decision, paragraph 61.
[123] IT SA Objection, p. 6.
[124] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 27 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 28.
[125] See paragraph 127 of this Binding Decision above.
[126] Draft Decision, paragraphs 67 and 211.
[127] IT SA Objection, p. 5.
[128] Draft Decision, paragraph 67.
[129] Draft Decision, paragraphs 80, 128.
[130] Draft Decision, paragraph 160.
[131] Draft Decision, paragraph 160.
[132] See this Binding Decision, paragraphs 127 and 183-184 above.

*187. The EDPB recalls that the concept of **context** relates to the circumstances of the processing[133]. The EDPB underlines that the processing at stake concerns personal data of a high number of particularly young children, i.e. children under 13 years old, in the context of their use of a social media platform.*

188. Article 24(2) CFR provides that 'in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration'[134]. The EDPB also recalls that, in accordance with Article 3(1) of the United Nations Convention on the Rights of the Child, 'the best interests of the child shall be a primary consideration'[135]. As pointed out both by the IE SA in the Draft Decision and by the IT SA in its objection, the GDPR recognises children as a vulnerable category of natural persons. This is displayed by a number of provisions in the GDPR[136]. In particular, Recital 38 GDPR states that children 'merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'[137]. Moreover, as raised by the IT SA[138], the GDPR, for instance its Article 8[139], envisages enhanced requirements for the processing of personal data of children under the age of 13 and in some cases, depending on Member State law, even for children of up to 16 years of age[140].

189. The consideration of the special protection guaranteed for children is particularly relevant in the present case as the TikTok platform is a social media service that is offered directly to children[141] - i.e. there is an offer of information society services directly to a child[142].

190. The EDPB also observes that the processing of personal data is at the core of the TTL business and the ban on access for below-13 child users to the TikTok platform is a fundamental precondition TTL is required to fulfil with a view to carrying out its

---

[133] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 27 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 28.

[134] Art. 24(2) CFR, also as referred to in the IT SA Objection, p. 5.

[135] Art. 3(1) of the United Nations Convention on the Rights of the Child (adopted by a resolution 44/25 of the General Assembly of the United Nations on 20 November 1989) stating that: 'In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration'.

[136] See also Judgment of the Court of Justice of 4 July 2023 in case *Meta Platforms et al v Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, paragraph 111.

[137] Draft Decision, paragraph 69; IT SA objection, p. 5.

[138] IT SA Objection, p. 5. The IT SA refers to Art. 8 GDPR.

[139] Art. 8 (1) GDPR. The EDPB also recalls that Art. 6(1)(f) GDPR, referring to the legal basis for processing consisting in the necessity for the purposes of the legitimate interests of the controller or a third party, raises in particular the case where the data subject is a child in the context of the balancing exercise to be carried out by the controller. The EDPB further recalls that, if a data subject is a child, this is also a relevant factor for the controller to take into account when relying on Art. 6(1)(b) GDPR, see EDPB Guidelines 2/2019 on Art. 6(1)(b) GDPR, paragraph 13.

[140] Art. 8(1) GDPR.

[141] IT SA Objection, p. 6.

[142] The EDPB recalls that, as TTL explicitly acknowledges, it offers the TikTok platform to users under 18 years of age (Draft Decision, paragraphs 12 and 13).

business[143]*. As the IT SA highlights, the company would have to otherwise discontinue its core business with all the related processing of personal data*[144].

191. *Moreover, as observed by the IT SA in its objection*[145]*, there have been numerous reports indicating possible dangers to children related to their use of the TikTok platform. These risks were also acknowledged by TTL in its DPIA* [redacted]

192. *The* ***purpose*** *pertains to the aims of the processing*[147]*. TTL provides the TikTok platform*[148]*. The Draft Decision states that 'TikTok is a video-focused social media platform that allows registered users to create and share videos of varying durations and to communicate with other users through messages'*[149]*. As submitted by TTL, it 'provided a global entertainment platform that, at its core, was designed to enable Users to create and share video content, enjoy videos from a variety of creators, and otherwise express their creativity, such as by interacting with videos to express new perspectives and ideas'*[150].

193. *This primary purpose informed the way in which the TikTok platform operated*[151]*, while TTL, as a private company, is pursuing commercial interest by carrying out the processing in the context of its services. In this respect, the EDPB observes that the number of users of the TikTok platform and the level of their engagement in the TikTok platform in relation to the processing at stake has relevance for commercial interests of TTL.*

'risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'

194. *As a general remark, the EDPB recalls that, when performing the risk analysis for compliance with Article 25(1) GDPR, the controller has to identify the* ***risks*** *to the rights of data subjects and determine* ***their likelihood and severity*** *in order to implement measures to effectively mitigate the identified risks*[152]*. A systematic and thorough evaluation of the processing is crucial when doing risk assessments. The controller must always carry out a*

[143] IT SA Objection, p. 7.
[144] IT SA Objection, p. 7.
[145] IT SA Objection, p. 6.
[146] TTL Children's Data and Age Appropriate Design DPIA, Risk n. 1 on p. 31 and Risk n. 6 on p. 38 (on p. 32 and 39, TTL describes the measures taken to mitigate these risks).
[147] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 27 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 28.
[148] Draft Decision, paragraphs 7 and 10.
[149] Draft Decision, paragraph 5.
[150] Draft Decision, paragraph 5, referring to TTL PDD Submissions, paragraphs 3.1-3.2.
[151] TTL PDD Submissions, paragraph 3.2.
[152] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 29 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 30.

data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards envisaged[153].

195. Therefore, in complying with the requirements of Article 25(1) GDPR, in the first instance, it is necessary to identify the risks to the rights and freedoms of data subjects that a violation of the data protection principles presents. The controller must have regard to the likelihood and severity of those risks and must implement measures to effectively mitigate them.

196. Recital 75 GDPR provides examples of risks to the rights and freedoms of natural persons. These risks may include physical, material or non-material damage to natural persons[154]*. Recital 76 GDPR provides guidance as to how risk should be evaluated, i.e. by reference to the nature, scope, context and purposes of the processing and on the basis of an objective assessment*[155]*. The EDPB recalls that the GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35 GDPR, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR*[156].

197. The EDPB takes note that TTL has conducted the risk assessment with regard to the use of the TikTok platform by Child Users. Schedule 2 to the TTL Children's Data and Age Appropriate Design DPIA[157] *sets out the risks identified, a description of the risk, an assessment of the risk level before any mitigations are put in place ('Inherent Risk'), the proposed mitigation measures to be put in place, and an assessment of the risk level after the relevant mitigations have been put in place ('Residual Risk'). The methodology for calculating the overall risk score for each risk is as follows: [redacted]. This is applied for both the Inherent Risk and the Residual Risk*[158].

---

[153] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 31 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 32.

[154] Recital 75 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 the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects' (emphasis added).

[155] Recital 76 GDPR.

[156] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 28 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 29, also stating that: '[t]he assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing)'.

[157] TTL Children's Data and Age Appropriate Design DPIA, Schedule 2.

[158] TTL Children's Data and Age Appropriate Design DPIA, Schedule 2, Part A.

198. *The TTL Children's Data and Age Appropriate Design DPIA identifies thirteen risks to Child Users[159]. These are:*

i. [redacted]

[redacted]

xiii. [redacted]

199. *As stated in the Draft Decision, TTL identifies* [redacted]. *In relation to its mitigation measures, TTL determines that* [redacted]. *However, the IE SA in the Draft Decision indicates that there is still a high risk in terms of likelihood and severity[162].*

200. *The EDPB takes note that TTL disagrees with that categorisation of the risk, as TTL considers that the risks outlined by the IE SA are potential and hypothetical risks at best and some of them are outside the scope of data protection law[163]. However, first, the EDPB notes that the IE SA's assessment of the level of the risk is not disputed by any of the CSAs*

[159] TTL Children's Data and Age Appropriate Design DPIA at Part B, Schedule 2; Draft Decision, paragraph 90.
[160] Draft Decision, paragraph 91.
[161] Draft Decision, paragraph 91.
[162] Draft Decision, paragraph 102
[163] TTL PDD Submissions, paragraphs 4.18-4.25.

and, secondly, the EDPB agrees with the IE SA's assessment in this respect and is not swayed by the arguments of TTL.

201. At the outset, the EDPB observes that in the Draft Decision the IE SA notes that TTL Children's Data and Age Appropriate Design DPIA [redacted] The EDPB considers that TTL's failure to specifically assess the risks for children under the age of 13 were they to get access to the TikTok platform has clear implications for TTL's ability to implement appropriate technical and organisational measures in accordance with Article 25(1) GDPR. As recalled above[165], the risk assessment is necessary in order to verify the required effectiveness and the appropriateness of the measures and safeguards envisaged.

202. The EDPB recalls that children are recognised as vulnerable persons under GDPR[166] and this case concerns processing of the personal data of particularly young children, i.e. under the age of 13. Further, the EDPB observes that TTL itself determines that even for users above 13 covered by TTL Children's Data and Age Appropriate Design DPIA, [redacted]

203. The EDPB agrees with the IE SA's remark that, with respect to Child Users, including children under the age of 13 who were to gain access to the TikTok platform, due to the relevant public features of the TikTok platform, the risks for Child Users include: loss of autonomy and control over their data, and possibly becoming targets for bad actors, given the public nature of their use of the TikTok platform; them becoming subject to a wide range of potentially deleterious activities, including online exploitation or grooming, or further physical, material or non-material damage where they inherently or advertently reveal identifying personal data; risk of social anxiety, self-esteem issues, bullying or peer pressure[170].

204. The EDPB also agrees with the IE SA's assessment that, while the risks identified in the TTL Children's Data and Age Appropriate Design DPIA apply equally to children under the age of 13 as those over the age of 13, the risks associated with these users are exacerbated and particularly severe given their young age and that the TikTok platform is expressly not intended for those under the age of 13[171]. Indeed, TTL explained that it offers the TikTok platform to users, who are 13 years old or older[172]. The TikTok platform has a

---

[164] Draft Decision, paragraph 96.
[165] See paragraph 195 of this Binding Decision above.
[166] Recitals 38 and 75 GDPR. See also WP29 Guidelines on DPIA, p. 9 stating that the processing of personal data of vulnerable data subjects, which may include children, is to be considered when assessing the existence of inherit high risk.
[167] Draft Decision, paragraph 91. Also, Part B of the TTL Children's Data and Age Appropriate Design DPIA.
[168] [redacted] TTL Children's Data and Age Appropriate Design DPIA, p. 31.
[169] TTL Children's Data and Age Appropriate Design DPIA, p. 32, 34, 36.
[170] Draft Decision, paragraph 93-94.
[171] Draft Decision, paragraph 96.
[172] Draft Decision, paragraph 12.

content rating on the Apple App store of '12+' and on the Google Play store of 'Parental Guidance Recommended'[173].

205. Furthermore, the EDPB concurs with the IE SA regarding the risks identified in the Draft Decision specifically for children under the age of 13 who were to gain access to the TikTok platform[174], *in particular the risk of viewing and accessing materials that are harmful or inappropriate for a child of such youth, particularly given that the TikTok platform is not intended for children under 13*[175].

206. The EDPB also recalls that in the Draft Decision the IE SA found that the public-by-default account setting exposes social media posts by Child Users to an indeterminate audience and that this presents a severe risk for Child Users[176]. *This is even more pertinent in relation to a significant number of children under the age of 13 who had access to the TikTok Platform for an undetermined period*[177].

207. Considering the above and taking into account the nature, scope, context, and purposes of processing, the EDPB shares the conclusion of the IE SA in its Draft Decision that the processing at stake poses high risks and that those risks associated with the processing analysed in the Draft Decision were high both in terms of likelihood and severity[178].

208. The above assessment is applicable both for the ex ante and the ex post measures.

'State of the art' and 'cost of implementation'

*209. Under Article 25(1) GDPR, the reference to '**state of the art**' imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market*[179]. *In this respect, the EDPB underlines that the principle of accountability is an overarching one and requires the controller to take up its responsibility in choosing the measures to be applied*[180].

210. In line with TTL's accountability obligations, TTL had an obligation to consider and assess the measures available in the market when choosing the age verification measures that it considered to be appropriate technical and organisational measures[181] *in accordance with Article 25(1) GDPR. When it comes to the evaluation of the state of the art, therefore, TTL has to be able to demonstrate in the particular case that it has assessed and takes into account the state of art measures regarding age verification in order to*

[173] Draft Decision, paragraph 12.
[174] As evident from paragraphs 183-184 above, a high number of children under 13 years old indeed had access to the TikTok platform during the Relevant Period.
[175] Draft Decision, paragraph 94.
[176] Draft Decision, paragraph 95.
[177] See paragraphs 183-184 of this Binding Decision.
[178] Draft Decision, paragraph 104.
[179] EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 19 and EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 19.
[180] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 64.
[181] Art. 5(2) and Art. 24 GDPR, Recital 74 GDPR.

secure effective implementation of the data protection principles and rights of data subjects.

211. First, the EDPB wishes to reply to TTL's submission that during the Relevant Period there was no regulatory guidance in place specifying what constitutes appropriate and effective age verification mechanisms[182]. In this regard, the EDPB refers to paragraphs 91-92 of this Binding Decision and recalls that the obligations of controllers stem directly from the GDPR. The application of controllers' obligations under Article 25(1) GDPR to take into consideration the state of the art is not conditional upon existence of any further regulatory guidance regarding the measures to be implemented in a particular case[183]. In addition, the fact that the supervisory authorities or the EDPB are working on the future guidelines in a relevant field does not affect the need for the controller to comply from the outset with its obligations stemming from the GDPR.

212. In any case, the EDPB highlights that there was relevant guidance by the EDPB on age verification in its Guidelines 05/2020 on Consent[184].

213. The IT SA describes in its objection the concept of requiring a trusted third party to verify the identity and age of the user and makes reference to the BSI PAS 1296:2018 standard[185]. The EDPB highlights that the concept of requiring a trusted third party to verify the identity and age of the user is long established in some Member States [186] and that the BSI PAS 1296:2018[187] existed during the Relevant Period. This standard of the British Standards Institution has provided a framework for age check systems and is relevant to assess the available measures for age verification during the Relevant Period.

214. Furthermore, the EDPB underlines that the issue of age verification is not a new issue nor an issue limited to the context of the protection of personal data[188]. The practices with regard to age verification in other fields have to be taken into account when assessing the question of what constitutes the 'state of the art' in the context of Article 25(1) GDPR[189].

---

[182] TLL Art. 65 Submissions, paragraphs 6.20-6.25.

[183] As the obligation stems directly from the GDPR. See also EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 10.

[184] EDPB Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1. published on 11 May 2020 (hereinafter, the **'EDPB Guidelines on Consent'**), see section 7.1.3. Further, the EDPB Guidelines on Data Protection by Design and by Default, V1.0 were adopted on 13 November 2019, i.e. prior to the Relevant Period, and EDPB Guidelines on Data Protection by Design and by Default, V2.0 were adopted on 20 October 2020.

[185] IT SA Objection, p. 6.

[186] For example, the German Postident service has been available at least since 2010: https://web.archive.org/web/20100314082647/http://www.deutschepost.de/dpag?tab=1&skin=hi&check=yes&lang=de_DE&xmlFile=link1015473_1014871.

[187] The British Standards Institution, PAS 1296:2018: Online age checking. Provision and use of online age check services. Code of Practice, published on 31 March 2018: https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice/standard.

[188] See Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) amended by Directive (EU) 2018/1808, in particular Art. 28b thereof which obliges the video-sharing platforms to, along the other things, establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors.

[189] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 22.

By way of clarification, the elements identified by the EDPB are not meant to be exhaustive.

215. The EDPB also points out that the state of the art is not statically defined at a fixed point in time, but should be assessed continuously in the context of technological progress. If a controller fails to keep up to date with technological changes, this could result in a lack of compliance with Article 25 (1) GDPR[190].

216. In reply to TTL's assertion that the age verification measures implemented by TTL during the Relevant Period compare, according to the expert report submitted by TTL, favourably to those of its competitors[191], *the EDPB points out that a particular controller's compliance with Article 25 GDPR is assessed on a case-by-case basis, taking into account the nature, context, scope and purpose of the processing at stake, as well as the risk to fundamental rights and freedoms of individuals in each specific case. Moreover, the potential infringement of the law by another party does not legitimise one's own infringement of the law. The EDPB is therefore not swayed by this argument.*

217. Taking into account the elements available to the EDPB in the context of this procedure the EDPB considers that, in this particular case, it does not have sufficient information to conclusively assess, pursuant to Article 25(1) GDPR, the state of art element in relation to measures implemented by TTL for the age verification of children as young as 13 years old during the Relevant Period.

*218. Finally, regarding the '**cost**' element in Article 25(1) GDPR, the EDPB recalls that the controller is not required to spend a disproportionate amount of resources when alternative, less resource-demanding, yet effective measures exist. However, the chosen measures need to ensure that the processing activity foreseen by the data controller does not process personal data in violation of the data protection principles, regardless of cost*[192].

219. The EDPB observes that in the present case TTL has not made any submissions demonstrating disproportionate cost for the implementation of the possible additional or alternative measures with regard to age verification on the TikTok platform. In any case, the EDPB agrees with the IT SA that a leading-edge technologically innovative company such as TTL that is addressing its social media services to children should be in a position to consider all available measures to ensure its compliance with Article 25 GDPR in an effective manner[193].

Whether the technical and organisational measures implemented by TTL with regard to age verification were 'effective'

220. The EDPB recalls that, as established in the Draft Decision[194], *TTL implemented the technical and organisational measures for age verification during the registration process*

[190] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 20.
[191] TTL Art. 65 Submissions, paragraph 6.28.
[192] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraphs 23-25.
[193] IT SA Objection, p. 7.
[194] Draft Decision, paragraphs 190-203.

to prevent children under the age of 13 from accessing the TikTok platform as described in paragraphs 124-125 of this Binding Decision above.

221. The EDPB notes that under Article 25(1) GDPR the requirement for the measures to be 'appropriate' means that the measures and necessary safeguards implemented by a data controller should be suited to achieve the intended purpose, i.e. they must implement the data protection principles enumerated in Article 5(1) GDPR 'in an effective manner'[195].

222. In light of the above, the EDPB proceeds to evaluate the effectiveness or contribution to the effectiveness of the technical and organisational measures implemented by TTL in the case at hand.

223. The EDPB recalls the principle of accountability and notes that TTL as the data controller in the present case is responsible for and has to be able to demonstrate its compliance with the data protection principles under Article 5(1) GDPR and other provisions of the GDPR[196]. The accountability principle requires the controller to 'demonstrate the effects of the measures taken to protect the data subjects' rights, and why the measures are considered to be appropriate and effective'[197], thus it puts focus on the element of demonstration. With regard to the protection of children's rights under the GDPR and determining whether children are actually affected, the controller needs to be able to demonstrate effective measures for ensuring that the processing of their personal data is in compliance with the data protection principles as discussed in detail subsequently.

224. Therefore, TTL is responsible to demonstrate that it has assessed the feasible alternatives and chosen appropriate measures for age verification taking into account all the elements listed in Article 25(1) GDPR. In particular, TTL is liable to demonstrate the effectiveness of the measures chosen in the particular case. This is particularly important when the demonstration of compliance is linked to the protection of vulnerable data subjects such as children.

225. As mentioned above, the analysis of effectiveness under Article 25(1) GDPR refers to the implementation of data protection principles, i.e. all the principles enshrined in Article 5 GDPR. The IT SA's objection mentions in particular the principle of data minimisation[198]. In this regard, the EDPB recalls that Article 5(1)(c) GDPR requires TTL to ensure that it only processes personal data that is adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. Per TTL's Terms of Service, users of the TikTok platform[199] must be at least 13 years of age[200]. Therefore, for the purpose of providing its service, i.e. the TikTok platform[201], TTL could only process personal data of

---

[195] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 8.
[196] Art. 5(2) GDPR and Recital 74 GDPR.
[197] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 87.
[198] IT SA Objection, p. 7.
[199] Regarding the purpose of the TikTok platform, see paragraphs 192-193 of this Binding Decision above.
[200] Draft Decision, paragraph 12.
[201] Draft Decision, paragraph 5, referring to TTL PDD Submissions, paragraphs 3.1-3.2. TTL PDD Submissions, paragraph 3.2: 'TikTok provided a global entertainment platform that, at its core, was designed to enable Users to create and share video content, enjoy videos from a variety of creators, and otherwise express their creativity, such as by interacting with videos to express new perspectives and ideas'.

users of at least 13 years of age[202]. TTL should have implemented technical and organisational measures to this end.

226. As noted above[203], a particularly high number of users below the age of 13 was able to gain access to the TikTok platform, therefore TTL processed a high volume of personal data of vulnerable data subjects, i.e. children under the age of 13, during the Relevant Period, even though it was not necessary for the purpose of providing its service. Considering such high volume of personal data accidentally processed by TTL, the EDPB shares the concerns of the IT SA[204] regarding the lack of effective implementation by TTL of the principle of data minimisation in the present case.

227. As outlined in paragraphs 182-208 of this Binding Decision above, in particular due to the nature of the processing that concerns children under 13 and the context being the accessibility of a social media platform for a high number of such children, who constitute particularly vulnerable data subjects requiring specific protection and considering the high risk posed by the processing at stake, the EDPB is of the view that a particularly high level of effectiveness[205] is necessary to meet the requirements of Article 25(1) GDPR. Taking this into account, the EDPB does not find that the situation analysed in the present case is such where a reduced level of effectiveness would be appropriate. The measures implemented by TTL need to be analysed bearing this in mind.

228. When considering the level of 'effectiveness' of the measures implemented by TTL, the EDPB first notes the view of the IT SA that the age gate can be 'easily dodged'[206]. The EDPB agrees that the factor that an age verification system can be 'easily circumvented' constitutes a relevant factor considering the effectiveness of the measures in place[207].

229. Second, the EDPB takes account of TTL's indication that 'if an individual entered a birth date which indicated that they were under 13, they were simply told they were ineligible for an account. By not explaining the reason for either presenting the age-gate or for preventing a potential user from creating an account, this ensured that individuals were not encouraged to provide an inaccurate birthdate'[208]. While the EDPB takes note of the age gate was presented in a neutral manner, it observes that such measure in itself does not ensure sufficient discouragement of individuals to not enter an inaccurate date of birth. As described above[209], the date of birth constitutes the only information a user needs to provide before receiving the prompt of non-eligibility. Therefore, it is not inconceivable that an individual younger than 13 could conclude that the date of birth would constitute the sole factor for assessing their eligibility to access the TikTok platform.

230. Additionally, as with methods based on obscurity, once a way of circumvention is known, this method can be easily shared with peers to facilitate them circumventing the

[202] Insofar as such processing of personal data is compatible with GDPR.
[203] See paragraphs 183-184 of this Binding Decision above.
[204] IT SA Objection, p. 7.
[205] The German Bundesgerichtshof held in I ZR 102/05 based on Döring/Günter, MMR 2004, 231, 234; that '[t]he reliability of an age verification system presupposed that it eliminates simple, manifest and obvious possibilities for circumvention'.
[206] IT SA objection, p. 5 and 7.
[207] See footnote 424 above.
[208] TTL Art. 65 Submissions, paragraph 6.39.
[209] Paragraph 124 of this Binding Decision above.

measure in place. Lastly, the EDPB takes note of the fact that the TikTok app was rated as 12+ in the Apple store[210]*, therefore an individual interested in getting access to the TikTok platform could easily infer that in order to access the TikTok platform they needed to enter a date of birth indicating that their age is higher than 12 years old.*

231. The EDPB also takes into account the [redacted] mechanism employed by TTL in combination with self-declaration. The mechanism in place in practice [redacted] any device to [redacted]. Without prejudice to the impact of the [redacted] in place on the considered effectiveness, the mechanism [redacted]. Therefore, it is not inconceivable that data subjects under the age of 13 concluded that their lack of eligibility [redacted] and to conclude that an [redacted].

232. Additionally, the [redacted] according to TTL Children's Data and Age Appropriate Design DPIA, constitutes [redacted][211], which in practice means a below 13 year old could [redacted]. Additionally, [redacted]. Once a user has signed up, for example, by [redacted], it would therefore not be relevant anymore. Therefore, the EDPB considers that the [redacted] does not substantially enhance the effectiveness of the ex ante age verification process.

233. The EDPB further points out that the Allen Report submitted by TTL itself notes[212] *that the EDPB Guidelines on Consent indicate that '[i]n some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor'*[213]*. However, TTL's own risk assessment [redacted]*[214]*. The Allen Report does not take note, however, of the following paragraphs of the EDPB Guidelines on Consent stating that: 'In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR. Trusted third party verification services may offer solutions, which minimise the amount of personal data the controller has to process itself'*[215]*. Therefore, the EDPB Guidelines on Consent make it clear that more proof or proof of a higher quality is appropriate in high-risks cases and refer to trusted third party verification services in this respect (a solution indicated by the IT SA in its objection*[216]*).*

234. Taking into account the above[217]*, with respect to 'effectiveness' of the ex ante measures implemented by TTL, the EDPB expresses serious doubts as to whether the self-verification by the user [redacted] was a sufficiently effective solution for such high risk processing. Additionally, the EDPB*

[210] Draft Decision, paragraph 190.
[211] TTL Children's Data and Age Appropriate Design DPIA, p. 19, 3.a.iii. The EDPB notes that the DPIA in question is dated 8 October 2020, therefore this duration seems to be applicable at least as of that moment.
[212] Allen Report, section 5.1.1.
[213] EDPB Guidelines on Consent, paragraph 135.
[214] See paragraph 125 of this Binding Decision.
[215] EDPB Guidelines on Consent, paragraph 137.
[216] IT SA Objection, p. 6.
[217] Paragraphs 194-208 of this Binding Decision.

expresses serious doubts as to whether TTL has demonstrated, as required by the accountability principle, measurable effectiveness of the implemented ex ante measures.

235. Concerning the ex post measures, the EDPB notes that the reporting system [redacted] It is to be further noted that this is not a [redacted]

236. The other ex post measure relies on the matching of [redacted]. This mechanism hinges on users under 13 years of age [redacted][9]. In cases where [redacted], such content moderation tools will not be effective. TTL also did not provide information that allowed it to demonstrate that the majority of matches indeed identified a user below 13 years of age or whether the system is susceptible for false positives, i.e. to demonstrate the accuracy of the algorithm.

237. Further, in line with the accountability principle, the EDPB notes that within the available materials and submissions TTL did not demonstrate that either of these checks and the [redacted] are done often and timely enough to minimise the time such accounts stay active on the TikTok platform, as could have been done with statistics of the duration between the creation of an account by a user under 13 years of age and the subsequent deletion of that account[220].

238. Considering the above analysis, the EDPB expresses doubts as to whether the ex post measures implemented by TTL during the Relevant Period ensured a high level of effectiveness.

<u>Whether the technical and organisational measures implemented by TTL were 'appropriate' pursuant to Article 25(1) GDPR</u>

239. As a final step for the analysis, the EDPB will consider whether the age verification measures implemented by TTL during the Relevant Period were appropriate in accordance with Article 25(1) GDPR[221].

240. The EDPB further notes that, in order to be considered 'appropriate', the technical and organisational measures for age verification chosen by controllers have to be compliant with the data protection principles under Article 5 GDPR, for example the

---

[218] See paragraph 125 of this Binding Decision.

[219] Draft Decision, paragraphs 196-198.

[220] The EDPB notes as well that some time could be needed to perform the [redacted] in line with Art. 22 GDPR, where relevant, which could be not due to an issue under Art. 22 GDPR, but the result of the *ex post* use of content moderation measures to remedy a shortcoming, i.e. the registration of a user with age below 13, of the *ex ante* measures.

[221] In this regard the EDPB takes note of TTL's view that the measures implemented need to lead to an appropriate level of effectiveness and certainty of assessing the age, and not an absolute level of certainty (TTL Art. 65 Submissions, paragraph 6.32). However, as evident from the assessment in the sub-section 5.4.2 of this Binding Decision, the EDPB is assessing the measures implemented by TTL not against an absolute level of certainty and effectiveness, but against an 'appropriate' level as envisaged in Article 25(1) GDPR.

principle of data minimisation under Article 5(1)(c) GDPR, and need to fulfil other requirements of the GDPR.

241. *When assessing whether the ex ante and ex post measures employed by the controller were, taking together and as a whole, appropriate for attaining the aim of preventing the children below 13 years of age to use TikTok platform, the EDPB takes into account the standard set by the CJEU. While measures may not be sufficiently reliable to prevent all persons under the permitted age from being accepted, the measures needs to significantly reduce the likelihood of such acceptance that would exist if that method were not used*[222]*. The EDPB expresses serious doubts in relation to whether TTL provided sufficient evidence as required by Article 5(2) GDPR for the measures in place to demonstrate that it did 'significantly reduce' the likelihood of children under the age of 13 from accessing and using the TikTok platform.*

242. *For the purposes of its assessment, the EDPB considers that the additional ex post measures in place by TTL do not as such prevent the registration of children under 13 years of age but instead mitigate shortcomings of the ex ante measures by removing accounts belonging to children under 13 years of age when they are identified as such. In this regard, theoretically an ex post measure with a high enough level of accuracy and short enough delay in the removal of identified users could exist*[223]*. However, the EDPB has serious doubts if in the case at hand the ex post measures in place provide for such a level of effectiveness that would mitigate the shortcomings indicated above of the ex ante measures*[224]*.*

Conclusion

243. *Taking into account the above, the EDPB expresses its* ***serious doubts regarding the effectiveness*** *of the age verification measures put in place by TTL during the Relevant Period, and more specifically regarding whether the combination of the ex ante and ex post measures implemented by TTL were sufficient to bring the effectiveness to the level required in this specific case, considering the severity of the risks and the high number of vulnerable data subjects affected.*

244. *However, taking into account the elements available to the EDPB in the context of this procedure, the EDPB recalls that it lacks conclusive information regarding the state of the art element in relation to age verification during the Relevant Period*[225]*. Therefore, the EDPB* ***does not have sufficient information****, in particular in relation to the state of the art element,* ***to conclusively assess TTL's compliance with Article 25(1) GDPR****. Consequently, the EDPB* ***is not in a position to conclude*** *that TTL infringed Article 25(1) GDPR.*

245. *In light of the serious doubts expressed regarding the effectiveness of the measures chosen by TTL, the EDPB requires the IE SA to modify the conclusion set out in paragraph 221 of the Draft Decision in the IE SA's final decision in the present case, by stating that it cannot be concluded in this case that the technical and organisational measures in respect*

[222] Judgement of the Court of Justice 17 October 2013 in case *Michael Schwarz v Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670, paragraphs 42 and 43.
[223] Without prejudice to future work of the EDPB or national SAs, such a method may in turn create risks for other fundamental rights.
[224] See paragraphs 225-234 of this Binding Decision above.
[225] See paragraph 217 of this Binding Decision above.

of the age verification processes themselves undertaken by TTL during the Relevant Period infringed the GDPR in light of the measures undertaken and the extent to which TTL sought to ensure its platform remained accessible only to those above the age of 13.

246. As a final remark, the EDPB recalls that the appropriateness of the technical and organisational measures that need to be implemented to comply with Article 25(1) GDPR is, due to their link to the state of the art and the possible changes of the relevant risks, regularly changing over time. This is particularly relevant in the field of age verification. A controller therefore has to periodically review whether the measures applied are still appropriate at the current moment, taking into account all the factors under Article 25(1) GDPR, considering their specific case at hand, in particular the level of risk. In addition, controllers need to ensure that any measure chosen is compliant with EU and Member State law, in particular the GDPR.

Conclusion

221. As set out above, the EDPB was unable to conclude, following its assessment on the merits of the objection raised by the Italian SA, that an infringement of Article 25(1) GDPR had occurred/was occurring during the Relevant Period in the particular circumstances of this Inquiry and by reference to the state of the art at the time. Accordingly, and as directed by the EDPB further to the Article 65 Decision, I find that it cannot be concluded, in this case, that the technical and organisational measures in respect of the age verification processes themselves undertaken by TTL during the Relevant Period infringed the GDPR in light of the measures undertaken and the extent to which TTL sought to ensure its platform remained accessible only to those above the age of 13.

H. ISSUE 3: ASSESSMENT AND CONSIDERATION OF MATTERS CONCERNING TRANSPARENCY PURSUANT TO ARTICLES 5, 12 AND 13 GDPR

H.1 Application of Articles 5, 12 and 13 GDPR

222. The GDPR requires that personal data must be processed *"lawfully, fairly and in a transparent manner in relation to the data subject"*.[226] Specific GDPR provisions are contained in Articles 12(1) and 13 GDPR regarding the information to be provided to data subjects. Article 12(1) GDPR addresses the quality of information to be provided to data subjects, as follows:

> *The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14...to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.* [...]

223. During the Relevant Period, TTL provided both a Privacy Policy,[227] and a summary of that Privacy Policy for users under the age of 18.[228]

224. Article 13(1) GDPR provides as follows:

[226] Article 5(1)(a) GDPR.
[227] TTL TikTok Privacy Policy.
[228] TTL TikTok Summary for Users U18.

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:

[...]

(e) the recipients or categories of recipients of the personal data, if any

225. Article 13(2) provides:

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

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

[...]

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

226. The Article 29 Working Party (the predecessor to the EDPB) published 'Guidelines on transparency under Regulation 2016/679', which were subsequently endorsed by the EDPB in May 2018.[229]

227. TTL has made various submissions regarding Articles 5, 12 and 13 GDPR in the Response to the Notice of Commencement and in the Submissions dated 14 April 2022, including:

"The GDPR's transparency requirements do not prescribe the method of providing the information stipulated in Articles 12 and 13 GDPR. Rather, the GDPR's transparency requirements impose comprehensive and prescriptive obligations in respect of the content of the information to be provided to data subjects. Subject to the broad principles set out in Article 12, controllers are afforded a degree of flexibility to implement the transparency requirements in a manner they consider appropriate.

Article 12(1) of the GDPR details the requirement for a controller to: "take appropriate measures to provide any information referred to in Articles 13 and 14 ... to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child".

Article 13 GDPR exhaustively and prescriptively lists the information that must be provided to a data subject at the time of collection of personal data from the data subject. There is an inherent tension between providing the level of detail required by the GDPR (e.g. under Articles 13) while also informing Users in different age groups of

[229] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679', WP 260 rev.01 (Revised 11 April 2018).

the relevant information in a clear, concise, and intelligible manner in accordance with Article 12".[230]

228. Further:

> *"Article 12(1) GDPR provides that the controller shall take appropriate measures to provide information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The clarity of this information is particularly important where it is being provided to younger Users. This is also reflected in Recital 58. TikTok provided information required under Article 13 GDPR to younger Users in a manner consistent with Article 12. TikTok delivered the required information in plain, simple language, and tailored it to all Users, including younger Users who were part of its audience. In particular, TikTok had regard to the A29WP guidelines on transparency under Regulation 2016/67954 ("Transparency Guidelines") in devising its approach".*[231]

H.2 Analysis and findings regarding TTL's compliance with Articles 5, 12 and 13 GDPR

Overview of Issues and Transparency Compliance

229. During the period of 29 July 2020 to 31 December 2020, in the course of the registration process, individuals were required to confirm they had read the Privacy Policy and the Terms of Service. Following passage through the age gate, the user inserted their phone number or email, beneath which it was stated that, by continuing, the individual agreed to TikTok's Terms of Service and that he/she had read TikTok's Privacy Policy. Both documents were hyperlinked and would navigate to their respective text in the in-app browser. To continue, users were required to select either 'Send code' or 'Next', depending on whether the user inserted a phone number or email below this text.

230. This navigated to the confirmation of phone number, if used, and the selection of a password and username.

231. These documents were further available on the platform on the settings page.[232]

232. TTL made available an under-18s summary of its Privacy Policy. This was accessible via the platform on the settings page alongside the full privacy policy. The under-18s summary was not provided at registration in the same manner that the Terms of Service and Privacy Policy was.

233. Both the Privacy Policy and under 18s summary provided subsections in relation to who TTL shares personal information with; data retention criteria and periods; and, data subject rights.[233]

234. TTL also had a 'Youth Portal', intended to provide account security information.[234]

235. TTL had an account named 'TikTok Tips', which provided videos on platform features, including privacy and safety such as choosing between a private and public account and controlling

[230] Response to the Notice of Commencement at [16.1]-[16.3].
[231] Response to the Notice of Commencement at [19.1].
[232] Response to the Notice of Commencement at [16.4].
[233] Response to the Notice of Commencement at [17.1]-[17.19] and [18.1]-[18.6].
[234] Response to the Notice of Commencement at [16.5].

comments. This information was also accessible via the 'TikTok Safety Centre'. TTL notes that the same videos are not necessarily available but there is a considerable overlap.[235]

236. TTL also had a portal for parents.[236]

237. TTL states that it did not engage in automated decision making referenced in Articles 22(1) and 22(4) GDPR and, therefore, did not provide information to data subjects in relation to this.[237]

238. I will now consider whether TTL has complied with two particular transparency obligations under the GDPR.

239. The first transparency obligation for consideration is whether Child Users were appropriately made aware (in a concise, transparent, intelligible and easily accessible form, using clear and plain language) by TTL as a user of the TikTok platform of the various public and private account settings in accordance with Articles 5(1)(a), 12(1), 13(1)(e), 13(2)(a) and 13(2)(f) GDPR; to be read in conjunction with Recitals 38, 39, 58, 60 and 61 GDPR, and whether Child Users are able to determine the scope and the consequences of registering as a user, whether public or private.

240. In this regard, TTL states that it provided information to its Child Users regarding the scope and the consequences of registering as a user, whether public or private, in the following ways:

    (a) Through its Privacy Policy, which was available during the registration process and in the settings and privacy tab;

    (b) Through its "Summary for Users U18";

    (c) Through 'just-in-time' notifications;

    (d) By presenting to Child Users their adjustable settings at the point immediately before they posted a video;

    (e) Through other in-product disclosures, such as switching audience settings for accounts, the presentation of video-level settings to the user each time they went to post a video, and 'nudges' when users upload their first video;

    (f) Through a series of TikTok videos that explained to users how certain key features of the service worked and what steps users could take to protect their privacy and safety; and

    (g) Through additional measures such as the 'Help Centre', 'Safety Centre', a Parent Portal and Youth Portal.

241. The second transparency obligation for consideration is whether Child Users were appropriately made aware by TTL as a user of the TikTok platform of the public default setting in accordance with Articles 5(1)(a), 12(1), 13(1)(e), 13(2)(a) and 13(2)(f) GDPR; to be read in conjunction with Recitals 38, 39, 58, 60 and 61 GDPR, and whether Child Users are able to determine the scope

[235] Response to the Notice of Commencement at [16.5] and Submissions dated 14 April 2022 at [121].
[236] Response to the Notice of Commencement at [16.5].
[237] Response to the Notice of Commencement at [17.21] and [18.8].

and the consequences of registering as a user, and specifically that their profile will be defaulted to public.

242. In this regard, TTL provided information to its Child Users regarding default account settings in the following ways:

(a) Through its Privacy Policy, which was available during the registration process and in the settings and privacy tab;

(b) Through its "Summary for Users U18";

(c) Through 'just-in-time' notifications;

(d) By presenting to Child Users their adjustable settings at the point immediately before they posted a video;

(e) Through other in-product disclosures, such as switching audience settings for accounts, the presentation of video-level settings to the user each time they went to post a video, and 'nudges' when users upload their first video;

(f) Through a series of TikTok videos that explained to users how certain key features of the service worked and what steps users could take to protect their privacy and safety; and

(g) Through additional measures such as the 'Help Centre', 'Safety Centre', a Parent Portal and Youth Portal.

243. In its Response to the PDD, TTL made further submissions in this regard:

> *A lay person's (including a lay younger User's) interpretation of these terms (to the extent a younger User could understand such terms as "indefinite number of persons"), is that they are covered by the terms "anyone" or "everyone". This terminology reflects the fact that these are "public" accounts. This is why TikTok opted to use this simple, clear terminology that could be readily understood by all Users, including younger Users, as referring to a wide audience that could go beyond registered Users.*
>
> [...]
>
> *The terms "public", "anyone" and "everyone" are "concise, transparent, intelligible and easily accessible". They provide younger Users with the relevant information in a manner which is more concise and descriptive than an expression like "indefinite number of persons" while, at the same time properly communicating the fact that the content would be made public. "Public", "everyone" and "anyone" are widely used and understood terms, and little to nothing appears to be gained by using "indefinite".*
>
> [...]
>
> *Further information in relation to the term 'anyone' was also made available in the Privacy Policy and U18 Summary, in line with a layered approach to transparency obligations which the DPC has acknowledged as a valid approach. The disclosures in*

the Privacy Policy – which was, at all times, linked in the account registration flow – and the U18 Summary (which is referred to in the Privacy Policy) further explain that this means 'anyone on the Platform' or 'anyone on TikTok' respectively. Therefore, TikTok disagrees with the DPC's statement that "both documents did not set out that a User with a public account's content would be accessible to an indefinite audience." These terms clearly include any person who is viewing content on the TikTok app or website.

The Privacy Policy noted that:

> *"If your profile is public, your content will be visible to anyone on the Platform and may also be accessed or shared by your friends and followers… " (emphasis added)*

[…]

It is submitted, therefore, that TikTok made clear to younger Users the categories of recipients or potential recipients of their personal data where they used a public account, i.e. anyone using TikTok / anyone on TikTok, in accordance with Article 13(1)(e) GDPR. These terms clearly include a person viewing content on the TikTok app or website.

[…]

The above information was provided to younger Users in a manner which complied with Article 12(1) GDPR as:

> *(A) it was provided in a concise and transparent form;*
> *(B) it was easily accessible as it was specifically brought to younger Users' attention at the most relevant time when making their decision, and younger Users had to interact with the relevant screens; and*
> *(C) TikTok used clear and plain language, given that the text in the notices conveyed key information to them regarding the potential categories of recipient and the main privacy implications, i.e. that the 'public', 'anyone' and 'everyone' could view their content. The information provided also made the distinction between a public account and private account clear (as the key consequence of posting with a public account was explained)*[238]

244. On 7 September 2022, TTL submitted the Marwick Report, which I have considered in full. As set out therein, the Report was concerned with two discrete questions posed by TTL, namely:

i. *Would a younger User understand the content of the Account Information Pop-Up and the First Post Pop-Up?*

ii. *Would a younger User, when joining TikTok or posting a video, understand the terms "public," "anyone," or "everyone," and the significance and consequences of those terms, including that information posted publicly will be widely accessible*

[238] Response to the PDD at [7.10]-[7.34].

online - having regard to both their background knowledge and the plain meaning of those terms? [239]

245. In summary, the Marwick Report states that, in relation to the first question:

i. Both are written in clear language that 13–17-year-olds can understand;

ii. 13–17-year-olds have sufficient understanding of privacy and digital literacy to interpret the pop-ups accurately and consequently make informed decisions about who can view and/or interact with their content;

iii. The pop-ups adhere to best practices when designing the language and placement of social media affordances for teenagers.

246. In relation to the second question, the Marwick Report states that:

(a) Young people are knowledgeable about the implications of posting "public" content online.

(b) This language appears in privacy curricula in use across the EU.

(c) In empirical studies, young people use the words "public," "anyone," and "everyone" when describing the implications of posting content that can be widely viewed online.

247. In relation to young people's understanding of privacy,[240] the Marwick Report states:

> [...] [C]*opious empirical studies suggest that young people care deeply about their online privacy and can articulate and thoughtfully discuss these concerns with researchers, parents, teachers, and peers.* [...]
>
> [...] *They deeply value the ability to control who can view their online information, which they consider to be central to their concepts of privacy.*
>
> [...]
>
> *Overall, these studies suggest that younger users have a strong understanding of privacy in social media; that they understand how to balance their desire to have private and public content; and that we should not consider younger users less capable of understanding privacy settings than older users, as this is empirically untrue.*[241]

248. In relation to digital competency and privacy education,[242] the Marwick Report states:

> [...] *Thus, young people in the EU almost universally receive instruction in digital competency and, more specifically, online privacy.* [...]

---

[239] TTL, Correspondence of 7 September at [1.4] and the Marwick Report at [10]. "*Account Information Pop-Up*" and "*First Pop-Up*" refers to the notifications in Images 1 and 6 below respectively.
[240] The Marwick Report at [19]-[23].
[241] The Marwick Report at [19], [20] and [23].
[242] The Marwick Report at [24]-[30].

> [...] *In addition to formal education, parents and caregivers have considerable influence on young people's privacy practices, and research indicates that parents in most households engage in informal types of privacy education.* [...]
>
> *In sum, throughout the EU, young people are exposed to both formal and informal privacy education that includes information about social media and digital privacy and the implications of having public or private accounts.*[243]

249. In relation to Child Users' understanding of the 'Public', 'Private', 'Anyone', and 'Everyone',[244] the Marwick Report states:

> *"Research demonstrates that young people understand the implications of having public social media accounts. They understand that different people may interact with their content depending on whether they choose for it to be "public" or "private." Scholars refer to this as interpersonal privacy. Studies repeatedly demonstrate that 13–17-year-olds have high levels of sophistication with interpersonal privacy.*
>
> *Specifically, studies have found that 13–17-year-olds understand that if they post content to social media, it is "public" and "anyone" or "everyone" may see it. [...]*
>
> *To summarize, empirical studies show that young people use the words "public," "anyone," and "everyone" when describing the implications of posting content that can be widely viewed online. The use of "anyone" and "everyone" in the above studies reflects a common-sense understanding among young people that they should consider the general public—including unregistered users of social media, or "strangers"—to be a potential audience when posting their content using a public account online. This is echoed by young people's deep awareness of online celebrities—who have public accounts—and the wide audiences they command. Indeed, a minority of younger users seek to gain such online attention and leverage public accounts to do so".*[245]

250. Finally, the Marwick Report states that Child Users respond to clear and simple language, and that the terms employed by TTL are so.[246]

Analysis

251. The issues for consideration relate to whether Child Users are able to determine the scope and the consequences of registering as a user, whether public or private, and specifically that their profile will be defaulted to public. Given their interrelated aspects, and the submissions of TTL, their examination will be taken together.

252. In this regard, these transparency obligations relate to whether or not Child Users were adequately informed of the implications of registering as a user and adequately informed as to the implications of public-by-default processing. TTL has set out a number of resources and information addressed to this. I note from the outset that many of these resources only or primarily arise subsequent to a Child User registering – for example, by presenting to Child Users their adjustable settings at the point immediately before they posted a video; and through other

[243] The Marwick Report at [28]-[30].
[244] The Marwick Report at [31]-[35].
[245] The Marwick Report at [31], [32] and [35].
[246] The Marwick Report at [36]-[38].

in-product disclosures, such as switching audience settings for accounts, the presentation of video-level settings to the user each time they went to post a video, and 'nudges' when users upload their first video. A number of those resources are separately accessible without, or prior to, registration, such as the Help Centre, Safety Centre, the Youth Portal, Parent Portal and TikTok videos viewable via the website.

253. The starting point for examining these issues is the Privacy Policy. In relation to the categories of recipients of a user's personal data, it states:

> *Who do we share your information with?*
> *We share your data with third party service providers who help us to deliver the Platform including cloud storage providers. We also share your information with business partners, other companies in the same group as TikTok (including TikTok Inc in the US which provides certain services for us in connection with the Platform), content moderation services, measurement providers, advertisers and analytics providers. We may share your information with law enforcement agencies, public authorities or with other third parties only where we are legally required to do so or if such use is reasonably necessary (for instance, to ensure your or someone else's safety). For more information, click here.*
>
> [...]
>
> *Public Profiles*
> *If your profile is public, your content will be visible to anyone on the Platform and may also be accessed or shared by your friends and followers as well as third parties such as search engines, content aggregators and news sites. You can change who can see a video each time you upload a video. You can also change your profile to private by changing your settings to 'Private account' in 'Privacy and safety' settings. If your profile is public, other users can use your content to produce and upload further content, for example, by creating a duet with your video.*

254. As well as the Privacy Policy, TTL also maintained a 'Summary for Users U18'. The purpose of this was to provide key points from the Privacy Policy for Child Users.[247] It states:

> *Other TikTok users - If your account setting is 'public', anyone using TikTok will be able to see your videos, and if they choose to, engage, download and share them including on other apps. There are lots of ways to adjust who can see your videos and interact with you on TikTok. See the "You're in control" section.*
>
> [...]
>
> *You have certain rights in connection with your data, including the right to access your data, delete it or change it. You also have control over your profile and content. Unless you change the settings from public to private, anyone on TikTok can see your account. To make your account private, go to your app settings, select 'Privacy and safety' and switch it to 'Private Account'.*
> *You can change the settings on your video before you post it, including whether it is public and you allow other people to comment, duet, react or download it. You should change these settings if you want to stop other people from doing any of these things with your videos.*

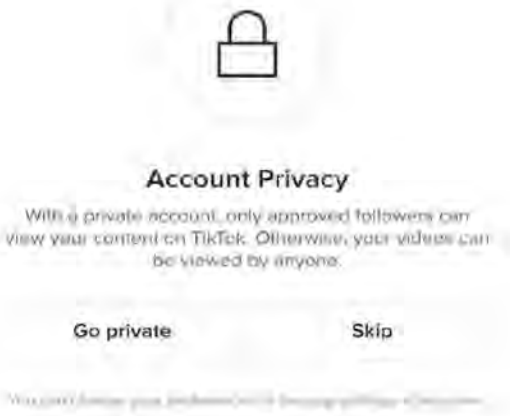
[247] Response to the Notice of Commencement at [11.2].

If you'd like to stop your profile being suggested to other TikTok users who are interested in accounts like yours, select 'Privacy and safety' and switch off 'Suggest your account to others'.

A step by step guide to adjusting all your privacy settings can be found here [https://www.tiktok.com/safety/youth-portal/define-your-public-presence?lang=en]

255. While both documents note that, where a user opts for a public account, the content posted on it is accessible to any other user, neither set out at all that, should any user have a public account, that account will be viewable via the TikTok website by an indefinite number of persons other than registered users.

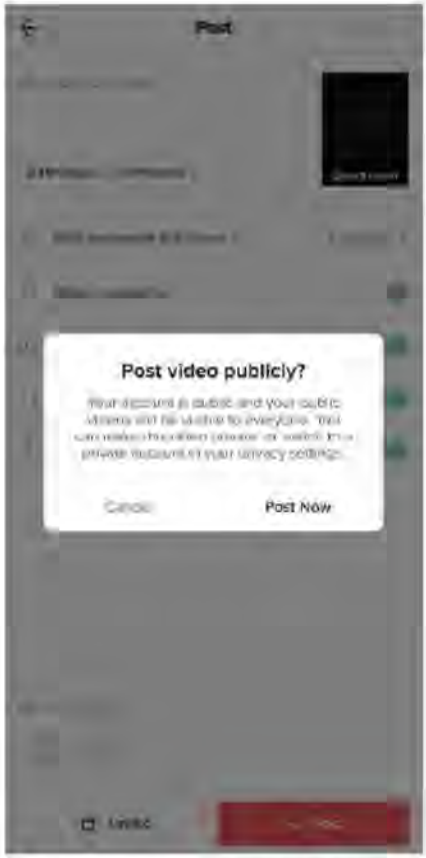
256. TTL also states that what it terms 'just in time' notifications were also utilised to ensure that it met its transparency obligations. In this particular context, TTL has set out the registration process and the variety of notifications relating to public and private account settings that it presents. TTL has set out the process for the registration of users in its various submissions. Upon downloading the mobile application, users were presented with the various options for opening an account using different credentials and were presented with links to the Privacy Policy and Terms of Service. Following successfully passing through the age gate, the relevant notification is as follows:



"Image 1 – nudge to switch to a private account"[248]

257. While the notification states that the videos of a Child User with a public account can be viewed by anyone, this notification does not indicate if this refers only to other registered TikTok users or indeed anyone at all. This notification did not allow a user to navigate to the Privacy Policy or the 'Summary for Users U18' in order to determine who "anyone" referred to and, in any event, even if they did (and indeed are linked in the initial screen) neither document set out that a user with a public account's content would be accessible to an indefinite audience, including unregistered users.

258. This is also indeed the case for whenever a user who had a public account chose to post a video:



"Image 6 Notification pop-up prior to posting a public video"[249]

259. TTL has also referred to its various portals and centres which help to ensure that it adhered to its transparency obligations. On the basis of the submissions made and an examination of those resources, none appear to make any reference to the fact that public accounts are viewable by non-registered persons.

260. I do not accept TTL's submissions that it used *"simple, clear terminology that could be readily understood by all Users"* and that the relevant references to the terms *"public"*, *"anyone"* and

[248] Response to the Notice of Commencement at 8 and Submissions dated 14 April 2022 at 30.
[249] Response to the Notice of Commencement at 11 and Image 2 in Submissions dated 14 April 2022 at 8. As noted in the Response to the PDD at Footnote 108, the Preliminary Draft Decision referred to an incorrect caption, which has been amended.

"everyone" are "concise, transparent, intelligible and easily accessible". Such terms are ambiguous insofar as they are capable of referring to both registered users and those not registered and this distinction could have been specified succinctly and easily. Indeed, per paragraph 7.20 of the Response to the PDD, TTL refers to Image 9 which states *"Anyone will be able to see your contents and likes. You will no longer need to approve followers."* This additional context would suggest that TTL was only referring to registered users, rather than anyone at all.

261. With regard to the Marwick Report, having considered it in full and the individual aspects that its conclusions rest upon, while I do not disagree with a number of its points, I am not persuaded with regard to its conclusions. First, in relation to young people's understanding of privacy, there is little that the report refers to in this regard that I would disagree with. It is not denied that young people have both a strong understanding of privacy and are desirous of ensuring control over their own privacy settings. I do not consider that young people are less capable of understanding privacy settings *per se*, nor that they do not care about their privacy, however, it is clear that, given the divergences in digital literacy across the European Union, discussed below, between different groupings, and on the basis of age, as well as the balance required to be placed between the value children place on privacy and that they also desire the ability to engage online,[250] the more necessary it is that the privacy implications of features are made clear and this in itself underlines the very central role and obligation of transparency in the GDPR. Simply because children are privacy-aware could not in itself mean the obligations under Articles 12 and 13 GDPR are satisfied, although awareness of the importance and function of privacy settings is of course, an important aspect of the objectives sought to be achieved by Articles 12 and 13 GDPR.

262. Second, with regard to the depth and extent of digital competency and privacy education around throughout the European Union, again I do not disagree that schooling across the European Union is increasingly incorporating digital competency and privacy into curricula. However, within the material relied upon and referenced in the Marwick Report it is clear that all authors are careful to note that the extent of such literacy and education is unevenly distributed across varying social, economic and geographic strata. Indeed, the Marwick Report refers to the *"EU Kids Online Survey"* (20 March 2020) primarily insofar as to state that 79% of children surveyed claimed to know how to change their privacy settings and 86% claimed to know what information they should and should not share.[251] However, the Marwick Report omits to note the emphasis in the following passage:

> *"Contrary to the myth of the digital natives, information navigation skills are unevenly distributed across the countries. These include the ability to assess the reliability of online information (varies between 36% and 75%) and the ability to choose the right keywords in an online search (varies between 52% and 89%), and are particularly low among children in Spain, Switzerland, Germany, France and Italy.*
>
> *The evidence counters another myth associated with the digital natives rhetoric and celebratory discourses of web 2.0 users as producers: children also vary greatly across*

[250] Livingstone, Stoilova, and Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review', London School of Economics and Political Science (January 2019) at 3, and Danah Boyd and Alice Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies' (A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford, England, 2011) at 25.

[251] Smahel, et al, 'EU Kids Online 2020: Survey Results from 19 Countries' (March 2020), available at https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-KidsOnline-2020-March2020.pdf

countries with respect to their levels of creative skills (varies between 55% and 86% in creating content and between 27% and 59% in editing content). Finally, while almost all the children know how to download an app on a mobile device, the management and monitoring of the costs of app use is unevenly distributed across the countries (varies between 48% and 84%)."

263. Further sources relied upon also highlight this crucial point. Per Livingstone, Stoilova, and Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review', London School of Economics and Political Science (January 2019), also cited by the Marwick Report:

> *"Not all children are equally able to navigate the digital environment safely, taking advantage of the existing opportunities while avoiding or mitigating privacy risks. The evidence mapping demonstrates that differences among children (developmental, socio-economic, skill-related, gender- or vulnerability-based) might influence their engagement with privacy online, although more evidence is needed regarding the consequences of differences among children. This raises pressing questions for media literacy research and educational provision. It also invites greater attention to children's voices and their heterogeneous experiences, competencies and capacities.*[252]

264. Indeed, Prof. Marwick has even noted this herself in Boyd and Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies' (A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford, England, 2011):

> *Even though all the teens we interviewed expressed an appreciation for privacy at some level, they did not share a uniform set of values about privacy and publicity. Just as some teenagers are extroverted and some introverted, some teens are more exhibitionist and some are more secretive. Variations among individuals are shaped by local social norms; sharing is viewed differently in different friend groups, schools, and communities.*[253]

265. Even leaving that aside, children are not a single monolithic category of data subject. Per Marwick and Boyd, 'Networked Privacy: How Teenagers Negotiate Context in Social Media':

> *Social media privacy controls imply that individuals should be held responsible for how they manage their privacy settings regardless of how well they understand those settings or how frequently those settings change* [...] *many users are not confident that they can configure their settings to obtain a desired level of privacy* [...] *Even when people do configure their settings correctly, information can still slip through the cracks.*[254]

266. Even in the premises that there is a link between disparate educational resources and the survey results relied upon by Prof. Marwick above and their relevance to the Inquiry, Recital 38 GDPR

---

[252] Livingstone, Stoilova, and Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review', London School of Economics and Political Science (January 2019) at 4.

[253] danah boyd and Alice Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies' (A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford, England, 2011) at 12.

[254] Alice Marwick and danah boyd, "'Networked Privacy: How Teenagers Negotiate Context in Social Media' 16(7) (2014) New Media & Society 1051–67 at 1062.

expressly provides that children merit specific protection because they may be less aware of risks. As the survey and other sources relied upon by the Marwick Report demonstrates, there are large divergences in the digital literacy of children across the European Union and the existence of various digital education initiatives does not, and could not, ameliorate TTL's obligations to more vulnerable Child Users under the GDPR. While on the level of generality it might be said that many children in some countries might have sophisticated levels of digital literacy and privacy education, this does not hold true for all and forms the very basis for the protections set out in the GDPR.

267. Third, with regard to Child Users' understanding of 'Public', 'Private', 'Anyone', and 'Everyone', the Marwick Report states that "*empirical studies show that young people use the words "public," "anyone," and "everyone" when describing the implications of posting content that can be widely viewed online*". This, paired with the report's previous submission regarding the understanding of privacy and the desire of young people to control their privacy, hits on a very critical aspect of this issue within the Inquiry and the indeed the very central thrust of Finding 5 in this Decision – it is absolutely central to a Child User's ability to control their privacy settings to be made aware of the implications of the decisions that they make. Indeed, the examples cited at paragraph 33 of the Marwick Report support this.

268. While the Marwick Report proceeds to state that "*the use of "anyone" and "everyone" in the above studies reflects a common-sense understanding among young people that they should consider the general public—including unregistered users of social media, or "strangers"—to be a potential audience when posting their content using a public account online*", I do not agree and it does not seem to be the case that this extrapolation of young people's understanding of those terms in different contexts necessarily supports the report's contention that the use of those words in the contexts provided within the Inquiry means Child Users would know they were referring to unregistered users of the relevant features in the world at large, rather than any registered user on the platform. In particular, the references cited do not differentiate in that regard and the literature relied upon does not reflect this, and the report refers only to those two notifications in isolation. The report does not make any detailed examination of this distinction, which is central to this issue. As the report so succinctly notes, Child Users have an often-extensive understanding of the differences between varying levels of privacy and are desirous of it. To that end, the failure to differentiate between any person at all and any registered user is central to this issue and it is within the specific context of the platform settings that this arises that is so critical.

269. The Marwick Report rightfully notes that Child Users respond to clear and simple language – as reflected in the GDPR – and again, no reason is provided why additional language explaining the implications of a public profile or the public publication of a video is not included, or the language used not expanded upon. I consider that TTL could have easily brought clarity to the fact that any unregistered person accessing the platform at all could view Child User's content.

270. In particular, it is worth noting again that the Privacy Policy, referred to in full above states that content would be visible to *"third parties such as search engines, content aggregators and news sites"*. There is no mention here at all of non-registered users. This is the critical context as to why the usage of the terms "*public*", *"everyone'"* and *"anyone"* was not sufficient. The reference to search engines is not sufficient as it does not necessarily follow that that non-registered users can access the content through the search engines without registering. Even at its height, a prudent and privacy-conscious Child User who consulted the Privacy Policy would have been unable to determine that any non-registered user at all could view their content. Article 13(1)(e) GDPR required TTL to provide information on the recipients or categories of

recipients of the personal data. This included information informing data subjects that non-registered users could view the content of public accounts. TTL did not provide any information for such recipients of the personal data. This forms the basis for that aspect of Finding 5, below, that pertains to the extent to which TTL can be said to have complied with Article 13(1)(e) GDPR.

271. With regard to that aspect of Finding 5, below, that pertains to the extent to which TTL can be said to have complied with its obligations under Article 12(1) GDPR, while TTL did provide some of the information required under Article 13(1)(e) GDPR regarding some recipients, that information was not provided in a manner that was concise, transparent and intelligible or in a form which was easily accessible, using clear and plain language. TTL used the word *"may"* in terms of the recipients that they did mention; "may" is a conditional term and I consider that the use of this term indicates that TTL did not communicate in a clear, plain and transparent manner to a Child User what recipients would definitely receive the Child User's personal data in each case. In addition, while TTL did inform users that content would be visible to some *"third parties"*, this was not found at all in their 'Summary for Users U18'. I consider that TTL therefore did not provide this information in an easily accessible form for Child Users. Finally, TTL did not explain precisely who might constitute a third party in this context. I consider that the use of an imprecise umbrella term such as "third parties" is unclear and opaque as it does not provide Child Users with specific information about the recipients of their personal data. In the circumstances, the language used in providing information required under Article 13(1)(e) GDPR was not clear and plain and was not provided in a concise, transparent and intelligible form. Furthermore, by failing to include any reference to third parties in the 'Summary for Users U18', the information that was provided was not provided in an easily accessible form. While the premise of the Marwick Report is that those terms, in themselves, may seem clear and comprehensible, this strips them of their context within the terms of both the platform settings themselves and with regard to the Privacy Policy and 'Summary for U18 Users'.

272. Accordingly, for these reasons, I do not accept the submissions set out in the Marwick Report, in this regard, and the conclusions flowing from them.

273. On this basis, I find that TTL failed to provide Child Users both with information as to the recipients or categories of recipients of personal data, as required by Article 13(1)(e) GDPR, so that they would be able to determine the scope and the consequences of registering as a user, whether public or private. Of the information that was provided by TTL – whereby there are various vague and opaque references to 'third parties', 'everyone' and 'anyone' as set out above – it cannot be said to have been provided in a manner that was concise, transparent, intelligible and in a form that was easily accessible, using clear and plain language. It was not clear at all if these references referred to all registered TikTok users or anyone who could access the platform via the website.

274. On this basis, plainly, as a direct result of the fact that all of these various resources and notifications failed to explain and/or to explain clearly the scope and consequences of public-by-default account settings, I further find that TTL failed to provide Child Users with information as to the fact that public-by-default processing of accounts meant that an indefinite audience, including non-registered users, would be able to view their personal data.

275. Article 5(1)(a) GDPR concerns the broader principle of transparency. However, it is important to emphasise that a finding of non-compliance with Articles 12 and 13 GDPR (or parts thereof) does not necessarily or automatically imply that there has been an infringement of Article 5(1)(a) GDPR. Nonetheless, there is a significant link between these principles. Indeed, transparency is an expression of the principles of fairness and accountability under the GDPR.

In this regard, I note that transparency is an *"overarching obligation under the GDPR"*[255] and is a broader expression of transparency than the specific obligations provided for in Articles 12 – 14 GDPR. Accordingly, while non-compliance with Articles 12 and 13 GDPR (or parts thereof) do not necessitate a finding of non-compliance with Article 5(1)(a) GDPR, in certain circumstances it is appropriate to find that there has been an infringement of both the specific transparency obligations and the broader principles of transparency where the extent of non-compliance with the former is sufficiently extensive to amount to an overarching infringement of the transparency principle. I note the EDPB's interpretation of this matter, as recorded in its Binding Decision 01/2021 ("**EDPB Binding Decision 01/2021**"),[256] which arose in the context of an inquiry conducted by the DPC for the purpose of examining the extent to which WhatsApp Ireland Limited complied with the transparency obligations set out in Articles 12, 13 and 14 GDPR. EDPB Binding Decision 01/2021 states, in this regard, as follows:

> *"188. The EDPB notes that the concept of transparency is not defined as such in the GDPR. However, Recital 39 GDPR provides some elements as to its meaning and effect in the context of processing personal data. As stated in the Transparency Guidelines, this concept in the GDPR "is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles". The key provisions concretising the specific practical requirements of transparency are in Chapter III GDPR. However, there are other provisions that also realise the transparency principle, for example, Article 35 (data protection impact assessment) and Article 25 GDPR (data protection by design and by default), to ensure that data subjects are aware of the risks, rules and safeguards in relation to the processing, as stated in Recital 39 GDPR.*
>
> *189. The EDPB also notes that transparency is an expression of the principle of fairness in relation to the processing of personal data and is also intrinsically linked to the principle of accountability under the GDPR. In fact, as noted in the Transparency Guidelines, a central consideration of the principles of transparency and fairness is that "the data subject should be able to determine in advance what the scope and consequences of the processing entails" and should not be taken by surprise about the ways in which their personal data has been used.*
>
> *190. Thus, it is apparent that, under the GDPR, transparency is envisaged as an overarching concept that governs several provisions and specific obligations. As stated in the Transparency Guidelines, "[t]ransparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights".*

[255] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' WP 260 rev.01 (Revised 11 April 2018) at [1].
[256] European Data Protection Board, 'Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (Adopted 28 July 2021).

191. This being said, it is important to differentiate between obligations stemming from the principle of transparency and the principle itself. The text of the GDPR makes this distinction, by enshrining transparency as one of the core principles under Article 5(1)(a) GDPR on the one hand, and assigning specific and concrete obligations linked to this principle, on the other one. The concretisation of a broad principle in specific rights and obligations is not a novelty in EU law. For example, with regard to the principle of effective judicial protection, that CJEU has stated that it is reaffirmed in the right to an effective remedy and to a fair hearing, enshrined in Article 47 of the Charter. Nonetheless, that does not imply that principles as such cannot be infringed. In fact, under the GDPR the infringement of the basic principles for processing is subject to the highest fines of up to 20.000.000€ or 4% of the annual turnover, as per Article 83(5)(a) GDPR.

192. On the basis of the above considerations, the EDPB underlines that the principle of transparency is not circumscribed by the obligations under Articles 12-14 GDPR, although the latter are a concretisation of the former. Indeed, the principle of transparency is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive. In addition, as stated above, Article 83(5) GDPR includes the possibility to find an infringement of transparency obligations independently from the infringement of transparency principle. Thus, the GDPR distinguishes the broader dimension of the principle from the more specific obligations. In other words, the transparency obligations do not define the full scope of the transparency principle.

193. That being said, the EDPB is of the view that an infringement of the transparency obligations under Articles 12-14 GDPR can, depending on the circumstances of the case, amount to an infringement of the transparency principle."

276. In the particular circumstances, I do not consider that TTL's informational deficits constitute an infringement of Article 5(1)(a). This is because, while the infringements of Articles 12(1) and 13(1)(e) GDPR are serious in nature, they are not of such a nature that they extend beyond the confines of those specific articles and are not sufficiently extensive to amount to an overarching infringement of the transparency principle. Specifically, and having regard to EDPB Binding Decision 01/2021, I do not consider that TTL's informational deficits are of the nature or extent described in EDPB Binding Decision 1/2021 such that it might be said that there has been an infringement of the Article 5(1)(a) GDPR transparency principle itself. While TTL ought to have informed the data subjects that non-registered persons could view their public accounts, having regard to the particular circumstances and the information that was provided, this informational deficit is confined to Articles 12(1) and 13(1)(e).

Finding 5

In circumstances where TTL did not provide Child Users with information on the categories of recipients or categories of recipients of personal data, I find that TTL has not complied with its obligations under Article 13(1)(e) GDPR.

In circumstances where TTL did not provide Child Users with information on the scope and consequences of the public-by-default processing (that is, operating a social media network which, by default, allows the social media posts of Child Users to be seen by anyone) in a concise, transparent and intelligible manner and in a form that is easily accessible, using clear and plain language, in particular insofar as the very limited information provided did not make it clear at all that this would occur, I find that TTL has not complied with its obligations under Article 12(1) GDPR.

I. ASSESSMENT OF WHETHER TTL INFRINGED THE ARTICLE 5(1)(A) PRINCIPLE OF FAIRNESS

277. During the course of the Article 60 consultation period, the Berlin SA (representing the views of the SAs of Berlin and Baden-Württemberg) raised an objection, the objective of which was to require the amendment of the Draft Decision to include a finding of infringement of the Article 5(1)(a) GDPR principle of fairness. The DPC decided that it was not in a position to follow the objection and, consequently, the DPC referred it to the EDPB for determination pursuant to Article 65(1)(a) GDPR. Having considered the matter, the EDPB determined as follows:

> *98. Moving forward with the assessment of the question raised by the DE SAs objection, the EDPB recalls that the basic principles relating to the processing listed in Article 5 GDPR can, as such, be infringed[257]. This is apparent from the text of Article 83(5)(a) GDPR which subjects the infringement of the basic principles for processing to administrative fines up to 20 million euros, or in the case of undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher[258].*
>
> *99. The EDPB underlines that the principles of fairness, lawfulness and transparency, all three enshrined in Article 5(1)(a) GDPR, are three distinct but intrinsically linked and interdependent principles that every controller should respect when processing personal data. The link between these principles is evident from a number of GDPR provisions: Recitals 39 and 42, Article 6(2) and Article 6(3)(b) GDPR refer to lawful and fair processing, while Recitals 60 and 71 GDPR, as well as Article 13(2), Article 14(2) and Article 40(2)(a) GDPR refer to fair and transparent processing[259].*
>
> *100. The EDPB highlights that the fairness principle has an independent meaning and stresses that the assessment conducted by the IE SA on TTL's compliance with the principle of transparency (leading to Finding 5 where the IE SA concluded that Article 13(1)(e) and Article 12(1) GDPR were breached, but the principle of transparency, pursuant to Article 5(1)(a) GDPR was not breached[260]) does not automatically rule out the need for an assessment of TTL's compliance with the principle of fairness too[261].*

[257] EDPB Binding Decision 3/2022, paragraph 218; Binding Decision 4/2022, paragraph 223; Binding Decision 5/2022, paragraph 141. See also Binding Decision 1/2021, paragraph 191.
[258] EDPB Binding Decision 3/2022, paragraph 218; Binding Decision 4/2022, paragraph 223; Binding Decision 5/2022, paragraph 141.
[259] EDPB Binding Decision 3/2022, paragraph 219; Binding Decision 4/2022, paragraph 224; Binding Decision 5/2022, paragraph 145.
[260] Draft Decision, paragraph 275.
[261] EDPB Binding Decision 3/2022, paragraph 220; Binding Decision 4/2022, paragraph 225; Binding Decision 5/2022, paragraph 147.

101. The EDPB has already provided some elements as to the meaning and effect of the principle of fairness in the context of processing personal data. For example, the EDPB has previously opined in its Guidelines on Data Protection by Design and by Default that '[f]airness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject'[262].

102. This definition, which was referred to by the IE SA when outlining 'the context of the processing' in the course of assessing TTL's compliance with Articles 24 and 25 GDPR including regarding the public-by-default processing of Child Users' social media content in the Draft Decision[263], highlights the importance of taking into account certain key elements in the practical implementation of the principle of fairness[264]. In particular, the elements of autonomy of data subjects, avoidance of deception, power balance, and truthful processing[265] are relevant in the case at hand.

103. Additionally, the EDPB has previously explained that 'the principle of fairness includes, inter alia, recognising the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller'[266].

104. The GDPR includes multiple references to the need for individuals to have control over their own personal data[267]. In this respect, the EDPB clarified that data subjects 'should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing'[268] and that controllers 'cannot present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data, or make it difficult for the data subjects to adjust their privacy settings and limit the processing'[269].

105. In addition, the EDPB noted in the past that the controller, in line with the fairness principle, must not present the data subjects with options in a way that 'nudges the data subject in the direction of allowing the controller to collect more personal data than if the options were presented in an equal and neutral way'[270]. The options to provide consent or abstain should be equally visible, and accurately representing the ramifications of each choice to the data subject[271].

---

[262] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 69, and EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 64.
[263] Draft Decision, paragraphs 77, referring to the EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraphs 69-70.
[264] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70.
[265] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70.
[266] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, adopted on 8 October 2019 (hereinafter, '**EDPB Guidelines 2/2019 on Article 6(1)(b) GDPR**'), paragraph 12.
[267] See the multiple references in GDPR, in particular in Recitals 7, 68, 75 and 85.
[268] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70.
[269] EDPB Guidelines on Data Protection by Design and by Default, V1.0, example 1 and V2.0, example 1.
[270] EDPB Guidelines on Data Protection by Design and by Default, V1.0, example 1 and V2.0, example 1.
[271] EDPB Guidelines on Data Protection by Design and by Default, V2.0, example 1.

106. It is also key to bear in mind that avoiding deception of the data subject means that 'Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design', while the element of truthfulness requires that 'The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects'[272].

107. Another important element of the fairness principle is linked to power balance[273], since the principle of fairness under Article 5(1)(a) GDPR underpins the entire data protection framework and seeks to address power asymmetries between the controllers and the data subjects in order to cancel out the negative effects of such asymmetries and ensure the effective exercise of the data subjects' rights[274]. It is relevant to recall that 'the personal data at issue related to a particularly vulnerable cohort of data subjects – children[275], who 'merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'[276]. Recital 75 GDPR explicitly includes the processing of individual's data particularly those of children, to be among the situations where the risk for the fundamental rights and freedoms of varying likelihood and severity, may result from data processing that could lead to physical, material or non-material damage. Along the same lines, children may qualify as 'vulnerable' data subjects, as they can be considered to not be able to knowingly and thoughtfully oppose or consent to the processing of their personal data[277].

108. It is therefore necessary for the EDPB to assess whether the two practices (i.e. the Registration Pop-Up and the Video Posting Pop-Up), which are the subject of the DE SAs' objection, are in line with the principle of fairness pursuant to Article 5(1)(a) GDPR.

109. The EDPB notes that, as detailed in the Draft Decision, all new TTL accounts, including Child User accounts, were set by default public[278], and that the IE SA considered that the information provided by TTL (which included the two pop-ups) did not allow Child Users to understand that their personal data would be visible to an indefinite audience (including non-registered users)[279]. More specifically, the EDPB finds it relevant that, according to the Draft Decision, the references to 'everyone' and 'anyone' in the information provided by TTL, which includes the Registration Pop-Up and the Video Posting Pop-Up, are 'vague and opaque'[280]. Moreover, the IE SA noted that the ambiguous terms of 'public', 'anyone' and 'everyone' were 'capable of referring to both

---

[272] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70, and EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 65.

[273] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70, and EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 65.

[274] EDPB Binding Decision 3/2022, paragraph 222; Binding Decision 4/2022, paragraph 227; Binding Decision 5/2022, paragraph 148.

[275] Draft Decision, paragraph 316.

[276] GDPR, Recital 38. See also Draft Decision, paragraph 69.

[277] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679 on 4 April 2017, WP 248 rev.1, (hereinafter **"WP29 Guidelines on DPIA")** endorsed by the EDPB on 25 May 2018, p. 10.

[278] Draft Decision, paragraph 128.

[279] Draft Decision, paragraph 273.

[280] Draft Decision, paragraph 272.

registered Users and those not registered'[281]. This means that the consequences arising from choosing one or the other option in the two pop-up notifications were not clear to Child Users[282].

110. This is all the more relevant considering that the IE SA acknowledged that 'where a Child User were to avail of the relevant public features of the TikTok platform there could lead in the first instance to Child Users losing autonomy and control over their data'[283]. In addition, the IE SA, stated that TTL 'failed to explain and/or to explain clearly the scope and consequences of public-by-default account settings' and moreover that 'TTL failed to provide Child Users with information as to that public by default processing of accounts meant indefinite audience, including not registered, would be able to view their personal data'[284].

111. Concerning, specifically, the Registration Pop-Up, the EDPB notes that, the IE SA's note that, this pop-up entailed the need for users to positively opt to choose a private account, since the option 'Skip' led to the account being set to public by default[285]. The consequence of omitting the decision by choosing 'Skip'[286] was to render the account public (as per the default setting) and thus to render the content viewable to an unlimited audience.

112. Moreover, as the IE SA states and as underlined by the DE SAs, the chosen language ('Skip') seems to 'incentivise or even trivialise the decision to opt for a private account' that the Child User was 'prompted' to make[287]. The DE SAs highlight that already this finding in the Draft Decision showed the use of 'nudging' during the registration process[288]. In addition, the IE SA also notes in its Draft Decision the fact that the decision to 'Skip' opting for a private account, has a cascading effect, in the sense that this would allow further platform settings to be rendered public[289]. According to a report of the Norwegian consumer authority, 'when the default settings allow widespread collection and use of personal data, users are nudged toward giving away their data'[290]. The DE SAs argue that 'Making it harder for data subjects to make a choice in favour of the protection of their personal data, rather than to the detriment of their data protection, constitutes an unfair practice and processing'[291]. The EDPB recalls that 'Data processing information

[281] Draft Decision, paragraph 259.
[282] Draft Decision, Finding 5, second part ('In circumstances where TTL did not provide Child Users with information on the scope and consequences of the public-by-default processing (that is, operating a social media network which, by default, allows the social media posts of Child Users to be seen by anyone) in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular insofar as the very limited information provided did not make it clear at all that this would occur, I find that TTL has not complied with its obligations under and 12(1) GDPR').
[283] Draft Decision, paragraph 93.
[284] Draft Decision, paragraph 173.
[285] Draft Decision, paragraphs 72 and 76.
[286] Draft Decision, paragraph 79.
[287] Draft Decision, paragraph 160. DE SAs Objection, p. 5.
[288] DE SAs Objection, p. 5
[289] Draft Decision, paragraph 173.
[290] Forbrukeradet, Report on deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy, dated on 27 June 2018, available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, p. 13.
[291] DE SAs Objection p. 6-7.

and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design'[292].

113. *The EDPB also highlights another feature of the Registration Pop-Up, namely the location of the option 'Skip' on the right side*[293]*. The DE SAs argue that the placement of an option on the right side will lead a majority of users to choose it, 'as internet and social media users are used to the button on the right side leading them to fulfil a step and go further (muscle memory)'*[294].

114. *Concerning the Video Posting Pop-Up, the EDPB agrees with the DE SAs that the 'nudging effect is amplified' by the fact that the option to post the video publicly is not only displayed on the right side, which has the effects mentioned above, but also shown in a bold darker text*[295]*. Consequently, as acknowledged by the IE SA, the settings plainly incentivised the selection of the posting of videos publicly, given both the phraseology used and the difference of colour gradient'*[296]*. In particular, the fact that the option to post the video publicly appears 'more visible and prominent' increases the likelihood for the user to choose it*[297]*. As noted by the DE SAs, also the 'muscle memory' and the location of the button leading to the 'more public' option raised the likelihood of the user choosing it*[298]*. This is essential, also considering the fact, that individuals, using digital services nowadays, on their phones while on the go, so forcing individuals to choose between several actions on the spot, is already a type of 'nudging'*[299]*, which can be even more efficient when the controllers 'emphasise; one of the two provided options.*

115. *As stated above, the EDPB recalls that 'options should be provided in an objective and neutral way'* [300] *and controllers should not 'present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data'*[301] *or 'nudges the data subject in the direction of allowing the controller to collect more personal data than if the options were presented in an equal and neutral way'*[302].

116. *Additionally, the Video Posting Pop-Up refers to the possibility of changing preferences in the Privacy settings*[303]*. The EDPB considers it relevant to highlight that this pop-up 'lacks a direct link to said settings', as mentioned by the DE SAs*[304]*. More specifically, this means that users who wish to change the settings will first need to select 'Cancel' and then go through the trouble of looking for the privacy settings, where they*

[292] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70; also EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 65.
[293] Draft Decision, Image 1.
[294] DE SAs Objection, p. 5.
[295] DE SAs Objection, p. 6. Draft Decision, paragraph 131 and Image 6 in paragraph 257.
[296] Draft Decision, paragraph 162.
[297] DE SAs Objection, p. 6.
[298] DE SAs Objection, p 5.
[299] Forbrukeradet, Report on deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy, dated on 27 June 2018, available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, p. 27.
[300] EDPB Guidelines on Data Protection by Design and by Default, V2.0, paragraph 70; also EDPB Guidelines on Data Protection by Design and by Default, V1.0, paragraph 65.
[301] EDPB Guidelines on Data Protection by Design and by Default, V1.0, example 1 and V2.0, example 1.
[302] EDPB Guidelines on Data Protection by Design and by Default, V1.0, example 1 and V2.0, example 1.
[303] Draft Decision, paragraph 257.
[304] DE SAs Objection, p. 6.

will then need to find the exact setting that concerns the visibility of the account/switching to a 'private account'[305]. The EDPB agrees, with the DE SAs, that this lowers the likelihood that data subjects change their settings, while there is a high likelihood that users will 'go along with posting the video with their pre-set settings'[306]. As mentioned above, controllers should not 'make it difficult for the data subjects to adjust their privacy settings and limit the processing'[307].

117. Based on all the above, the EDPB agrees with the DE SAs that the Registration Pop-Up and the Video Posting Pop-Ups were 'nudging the user to a certain decision'[308] and leading them 'subconsciously to decisions violating their privacy interest'[309]. It is relevant to consider, in this regard, that such decision towards which the users were encouraged is the 'public-by-default setting', which 'appears to be a deliberate choice on the part of TTL intended to maximise user engagement and sharing on the platform'[310]. The EDPB also concurs with the DE SAs that 'Making it harder for data subjects to make a choice in favour of the protection of their personal data, rather than to the detriment of their data protection, constitutes an unfair practice and processing'[311]. This is, in this case, combined with the fact that data subjects are children, who 'merit specific protection with regard to their personal data'[312], and with the lack of clarity as to the consequences of the different options particularly with regard to the audience of the future content of their account.

*118. On the basis of the findings of the IE SA in its Draft Decision and considering the arguments provided by the DE SAs in their objection, **the EDPB finds that TTL has infringed the principle of fairness, pursuant to Article 5(1)(a) GDPR**, in the context of the practices described above, namely the Registration Pop-Up and the Video Posting Pop Up.*

119. Accordingly, the EDPB instructs the IE SA to include in its final decision a finding of an infringement of the principle of fairness principle pursuant to Article 5(1)(a) GDPR by TTL.

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

Finding 6:

For the reasons established by the EDPB in the Article 65 Decision, TTL has infringed the principle of fairness pursuant to Article 5(1)(a) GDPR.

[305] DE SAs Objection, p. 6.
[306] DE SAs Objection, p. 6.
[307] EDPB Guidelines on Data Protection by Design and by Default, V1.0, example 1 and V2.0, example 1.
[308] DE SAs Objection, p. 4.
[309] DE SAs Objection, p. 8.
[310] Draft Decision, paragraph 72.
[311] DE SAs Objection p. 6-7.
[312] GDPR, Recital 38.

J. CORRECTIVE POWERS

279. I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my findings that TTL has infringed the following articles of the GDPR in respect of its data protection by design and default in respect of its processing of the personal data of Child Users: Articles 5(1)(c), 5(1)(f), 24(1), 25(1) and 25(2) GDPR.

280. I have also set out above my findings that TTL has infringed the following articles of the GDPR in respect of it age verification measures: Article 24(1) GDPR.

281. I have also set out above my findings that TTL has infringed the following articles of the GDPR in respect of its transparency obligations: Articles 12(1) and 13(1)(e) GDPR.

282. 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 data 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.

283. 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…*

284. Having carefully considered the infringements identified in this Decision, I have 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 I have decided are appropriate to address the infringements in the particular circumstances of this Inquiry are as follows:

    (a) An order pursuant to Article 58(2)(d) to TTL to bring its processing into compliance with the GDPR in the manner specified below;

    (b) A reprimand pursuant to Article 58(2)(b) of the GDPR; and

    (c) Three administrative fines in the range of €55 million to €100 million, €55 million to €100 million, and €110 million to €180 million, respectively.

285. I set out further detail, below, in respect of each of these corrective powers that I will exercise and the reasons why I have decided to exercise them.

286. For the avoidance of doubt, when the EDPB determined, by way of the Article 65 Decision, that this Decision must include a finding of infringement of the Article 5(1)(a) GDPR principle of fairness, it made a further determination in relation to the exercise of a corresponding corrective power. That further determination has been incorporated into this Decision, below.

K. ORDER TO BRING PROCESSING INTO COMPLIANCE

287. Article 58(2)(d) GDPR provides that a supervisory authority shall have the power:

"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"

288. In circumstances where I have found that the processing at issue was not in compliance with the GDPR, I will make an order pursuant to Article 58(2)(d) GDPR. In particular, I will order TTL to bring the relevant processing into compliance with Article 5(1)(c), Article 24(1), Articles 25(1) and (2), Article 12(1), Article 13(1)(e) GDPR and, as instructed by the EDPB in paragraph 280 of the Article 65 Decision, Article 5(1)(a) GDPR. The order under Article 58(2)(d) applies to the extent (if any) that TTL is conducting ongoing processing operations as described in this Decision.

289. Specifically, to the extent that TTL is engaged in ongoing public-by-default processing as described, this order requires TTL to take the following action:

(a) to implement appropriate technical and organisational measures in respect of any ongoing public-by-default processing, to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This order is made further to Findings 1 and 2 to ensure compliance with Article 5(1)(c), Article 24(1) and Article 25(1) and (2) GDPR.

(b) to provide Child Users with information in a clear and transparent form on the purposes of the public-by-default processing. This order is made further to Finding 5 and to ensure compliance with Article 12(1) and 13(1)(e) GDPR.

(c) to bring its processing, in the context of the Registration Pop-Up and the Video Posting Pop-Up of the TikTok platform, into compliance with the principle of fairness in accordance with Article 5(1)(a) GDPR, further to the instruction of the EDPB, as set out at paragraph 280 of the Article 65 Decision. Specifically, TTL is required to eliminate the deceptive design patterns identified in paragraphs 109-113 and 114-116 of the Article 65 Decision, taking into account the EDPB's analysis in paragraphs 104-107 and 117-118 of the Article 65 Decision.

290. My decision to impose the order is made to ensure that full effect is given to TTL's obligations under these articles. I consider that this order is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

K.1 Additional service modifications since the Relevant Period

291. In its Submissions dated 14 April 2022, TTL has submitted that additional changes have occurred with respect to its platform settings and approaches to age verification and transparency since the Relevant Period.

292. With respect to platform settings at registration, TTL states that, from January 2021, under-16 users were no longer required to make the choice during the account registration process to choose a private account or skip the private account option. Instead, these Child Users' accounts are defaulted to private, without any ability for these Child Users to choose a public account during the registration process. These Child Users are informed through a pop-up notification during the registration process that their account has been set to private.[313]

[313] Submissions dated 14 April 2022 at [76].

293. Further, from January 2021, the 'Duet' and 'Stitch' feature was disabled for all under-16 users, meaning that other users cannot 'Duet' or 'Stitch' with videos created by under-16 users. By default, only "Friends" of users aged 16 or 17 can make 'Duets' and 'Stitches' of videos created by these users. From January 2021, under-16 users do not have the option of allowing their videos to be commented on by "Everyone" and can only choose to receive comments from "Friends" or "No One". From January 2021, for Child Users aged 16 or 17, the download feature was turned "off" by default. Finally, from January 2021, the 'Suggest Your Account to Others' setting is turned off for under-16 users by default.[314]

294. With respect to transparency, TTL states that, since January 2021, Child Users under 16 are no longer given the option during the account registration process to make a choice in this regard and, instead, are defaulted to a private account and Child Users under 16 are accordingly now informed through a pop-up notification during the registration process that their account has been set to private and that only approved users can view their video. The pop-up notification also informs them that they can review and manage their account in their app settings.[315]

295. Finally, with respect to age verification measures, TTL states that it is currently proposing to build a [redacted][316]

296. In its Response to the PDD, TTL provided an Annex setting out the changes that have taken place since the Relevant Period and further submits that the order is extremely broad and it is unclear whether the order in fact requires that TTL take any specific actions and, if so, what form such actions should take and submits that it is not necessary to impose an order to bring processing operations into compliance in the Inquiry.[317]

K.2 Conclusion on the order to bring processing into compliance

297. I consider that the order detailed above is necessary to ensure that full effect is given to TTL's obligations in relation to the infringements outlined above. The substance of this order is the only way in which the defects identified in this Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that I am of the view that this power should be exercised.

298. In my view, such an order is proportionate and is the minimum order required in order to guarantee that compliance will take place in the future. The fact that TTL has started to take steps to bring its information into compliance reduces the practical impact of the order on the data controller's resources. On that basis, I am satisfied that the order is a necessary and proportionate action.

299. Insofar as TTL has made changes to its processing since the Relevant Period, then the order applies only insofar as is necessary to bring TTL's processing into compliance with the above stated provisions of the GDPR. As the relevant provisions, and indeed the GDPR itself, does not prescribe a particular form or manner of processing, it is incumbent on TTL to ensure compliance and I cannot dictate what form such actions should take. I am however cognisant that any order made pursuant to Article 58(2)(d) GDPR should order that processing operations

[314] Submissions dated 14 April 2022 at [3.5].
[315] Submissions dated 14 April 2022 at [128].
[316] Submissions dated 14 April 2022 at [140].
[317] Response to the PDD at [8.6]-[8.8] and Annex 1.

are brought into compliance with the GDPR "*where appropriate, in a specified manner and within a specified period*". Plainly, in order for TTL to bring its processing into compliance with the relevant GDPR provisions, to the extent that the processing outlined in this Decision continues to fail to be in compliance with the provisions of the GDPR, this processing should be brought into compliance.

300. This order should be complied with within three months of the date on which this Decision is notified to TTL, given the significant financial, technological and human resources at TTL's disposal, and taking into account, as noted above, that TTL has, since the Relevant Period, implemented a number of apposite changes. In relation to the deadline for compliance with that part of the order that corresponds to the finding of infringement of the Article 5(1)(a) GDPR fairness principle, I note that the EDPB has, at paragraph 280 of the Article 65 Decision, recorded that the "*specified timeframe*" for compliance above is "*to be determined by the [DPC]*". I further note, in this regard, that the EDPB described, at paragraph 280 of the Article 65 Decision, the requirement for the identified corrective action as an 'expansion' of the original compliance order that was proposed by the Draft Decision. Accordingly, and having regard to the significant financial, technological and human resources at TTL's disposal, I consider that all aspects of the corrective order set out above should be subject to a deadline for compliance of three months, commencing from the date on which this Decision is notified to TTL. I note that TTL did not, as part of its Final Submissions, make any submissions that disagreed with my proposal to apply a three-month deadline for compliance with that aspect of the above order that corresponds to the determination made by the EDPB at paragraph 280 of the Article 65 Decision.[318] I therefore require TTL to comply with the above order within three months of the date on which this Decision is notified to TTL. Further to this, I require TTL to submit a report to the DPC within that period, detailing the actions it has taken to comply with the order.

Additional Matters

301. For the avoidance of doubt, the order to bring processing into compliance detailed above takes account of TTL's Final Submissions, in which TTL identified a typographical error in the corresponding text of the Draft Decision. Further to those submissions, the first limb of the order has been amended to correctly refer to Findings 1 and 2 (in circumstances where the Draft Decision referenced Findings 1 and 3 in error). I note that the above order does not reference Finding 3 in circumstances where the platform setting which allowed non-Child Users to enable direct messaging for Child Users above the age of 16 was updated in or around mid-November 2020.[319] This meant that, from mid-November 2020 onwards, the non-Child User only had the power to disable the direct message function entirely if a Child User above the age of 16 had enabled it.[320] In the circumstances, I do not consider it necessary to require TTL to take action, as part of the order to bring processing into compliance, in response to Finding 3.

302. Furthermore, and for the sake of clarity, the above order also does not reference Finding 4 in circumstances where that finding concerns TTL's failure to properly take account of the risks posed by the specified processing and therefore its failure to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the specified processing was performed in accordance with the GDPR, contrary to Article 24(1) GDPR. For the avoidance of doubt, I consider that the remedial action that TTL is required to take pursuant to the terms of the order set out above will likely also bring about the rectification of the

[318] The Final Submissions at [3.6].
[319] Response to the PDD at [5.133]; the Final Submissions at [7.6.4].
[320] *Ibid.*

shortcomings identified by Finding 4. Consequently, I do not consider it necessary to specifically address Finding 4 within the terms of the order itself.

L. REPRIMAND

303. Article 58(2)(b) of the GDPR provides that a supervisory authority shall have the power:

> *"to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation"*

304. With regard to this, in its Response to the PDD, TTL submitted that I should revise the preliminary findings of infringement in light of the clarifications and information provided and if no finding of infringement is made, the question of a reprimand does not arise.[321] For the reasons set out in detail in relation to each finding above, I do not accept this.

305. I have decided to impose a reprimand on TTL for the infringements identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. Each of the infringements concern the personal data of a significant number of Child Users and are serious in nature. Reprimands are appropriate in respect of such non-compliance in order to formally recognise the serious nature of the infringements and to dissuade such non-compliance.

306. The reprimand is necessary and proportionate in addition to the order in this Decision. While the order would require specific remedial action on the part of TTL, the reprimand formally recognises the serious nature of these infringements. I consider that it is appropriate to formally recognise the serious nature of the infringements with a reprimand in order to deter future similar non-compliance by TTL and other controllers or processors carrying out similar processing operations, in particular in respect of the processing of children's data. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that TTL and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations regarding transparency, and data protection by design and by default.

M. ADMINISTRATIVE FINE

307. 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"*

308. This makes clear that the DPC may impose administrative fines in addition to, or instead of, the order and reprimand 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) GDPR.

309. Article 83(1) GDPR provides that:

> *"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*

[321] Response to the PDD at [8.3].

paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive."

310. 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.*

311. 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) GDPR. Therefore, I will now proceed to consider each of these factors in turn in respect of each of the individual infringements identified in this Decision.

312. In applying the Article 83(2)(a) to (k) factors to the infringements, I have set out below my analysis of the infringements collectively where it is possible to do so. However, in some instances it is necessary to set out each infringement individually in order to reflect the specific circumstances of each infringement and the factors falling for consideration. Regardless of whether the analysis below is individual or collective in respect of a particular factor or infringement, I have considered every infringement separately when deciding whether to impose an administrative fine in respect of each infringement. I have made a separate decision on each infringement, and I have made each decision without prejudice to any factors arising in respect of the other infringements. For the avoidance of doubt, my decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine where applicable, is independent and specific to the circumstances of each particular infringement. I note in this context that, regarding the infringement of Article 24(1) GDPR, this article is not among the provisions that are subject to Article 83. Article 83(1) GDPR refers to the power of supervisory authorities to impose administrative fines "*in respect of infringements*

of [the GDPR] referred to in paragraphs 4, 5 and 6". While this Decision records findings of infringement of Article 24(1) GDPR, that provision is not referred to in Articles 83(4), (5) or (6) GDPR. Therefore, it is not possible to impose an administrative fine in respect of the infringements of Article 24(1) GDPR. Accordingly, I have not considered the application of the Article 83(2) factors to the infringement of Article 24(1) GDPR.

M.1 Article 83(2)(a) GDPR: 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

313. In considering the nature, gravity and duration of TTL's infringements, I have had regard to the analysis in this Decision concerning the nature, scope, context and purposes of the processing. Article 83(2)(a) GDPR requires that I take these matters into account in having regard to the nature, gravity and duration of the infringements. Article 83(2)(a) GDPR also requires me to take into account the number of data subjects affected by the infringements and the level of damage suffered by them. Therefore, I will first consider these issues before proceeding to consider the nature, gravity and duration of the infringements.

314. TTL indicated that, during the period of 29 July 2020 to 31 December 2020, the approximate total average number of registered EU TikTok users under the age of 18 was [redacted] The approximate total average number of monthly EU TikTok users under the age of 18 was [redacted][322] TTL does not retain data to determine the approximate number of TikTok users that were identified as being under the age of 13 when attempting to register during the period from 29 July 2020 to 31 December 2020; however, TTL believes that the approximate number of individuals in the EU who failed registration on the basis of their identifying as an individual below 13 years of age during the equivalent number of days from 14 April to 16 September 2021 was [redacted].[323] During the period of 29 July 2020 to 31 December 2020, the approximate number of EU TikTok users that were detected as being under 13 subsequent to their registration and removed from the platform was [redacted]

315. TTL does not hold statistics on users' account status beyond [redacted] however, the approximate daily average number of EU TikTok users under the age of 18 with a private account at 23:59 hours on a given day between 14 September 2021 to 14 October 2021 was [redacted][325] TTL does not retain information on the approximate number of persons under the age of 18 that operated a public TikTok account during the period from 29 July 2020 to 31 December 2020; however, the approximate daily average number of EU TikTok users under the age of 18 with a public account at 23:59 hours on a given day between 14 September 2021 to 14 October 2021 was [redacted][326]

316. In its Response to the PDD, TTL made the following submissions:

> *"TikTok submits that Article 83(2)(a) GDPR makes clear that the number of data subjects impacted is not a relevant consideration in isolation and must instead be considered in light of any damage suffered by them. Notably, Article 83(2)(a) GDPR is*

[322] TTL initially indicated this number was [redacted] in Response to the Notice of Commencement at [9.2.1]-[9.2.2.]; however, in the Submissions dated 14 April 2022, at Annex A, it revised this downward to take into account users who turned 18 during the Relevant Period.
[323] Response to the Notice of Commencement at [9.2.3].
[324] Response to the Notice of Commencement at [9.2.4].
[325] Response to the Notice of Commencement at [9.2.5].
[326] Response to the Notice of Commencement at [9.2.6].

clear that only "damage suffered" is a relevant consideration and not the risks that may or may not have been present. In this regard, TikTok notes that there is no evidence that any actual damage has been suffered by younger Users as a result of the processing that is the subject of the Inquiry.

[...]

The DPC has primarily relied on assertions as to alleged loss of control and potential for younger Users to be subject to a number of speculative general risks arising from the use of the Platform which the DPC describes as a range of "potentially deleterious activities". TikTok acknowledges that risks such as grooming, online exploitation, bullying or peer pressure are risks that arise for individuals in the context of the online world. However, such risks cannot be ascribed to an alleged loss of control arising from the processing that is the subject of the Inquiry. As highlighted by the submissions in section 9.15(D) above, the DPC's position is speculative and is not supported by any evidence."[327]

317. In assessing the level of damage suffered by the data subjects, I have had regard to the loss of control suffered by them over their personal data. Regarding transparency, Articles 12(1) GDPR and 13(1)(e) GDPR empower data subjects to make informed decisions about engaging with activities that cause their personal data to be processed, and making informed decisions about how to exercise their rights. 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. TTL's infringements of Article 12(1) GDPR and Article 13(1)(e) GDPR regarding the public-by-default processing prevented Child Users from exercising control over their personal data. The minimal information in the registration process on the difference between public accounts and private accounts inhibited those children from choosing to make their accounts private. While it was open to them to opt into such a private account, the lack of information on the specific purpose of the default processing in the registration process and the Privacy Policy itself made it more difficult to understand the difference between public and private accounts and how to switch. By making it more difficult for children to make their accounts private, TTL restricted their choice and denied them control over their personal data. I find that this loss of control represents a significant amount of damage to the data subjects.

318. A core element of the principles of data minimisation and data protection by default in Articles 5(1)(c) and 25(1) and (2) GDPR requires controllers to ensure that they only process personal data that are necessary for each specific purpose. Data subjects are denied control over their personal data where a data controller processes it in a manner that is not necessary in relation the purposes of the processing. TTL's infringements of Articles 5(1)(c) and 25(2) GDPR affected each of the data subjects because TTL failed to ensure that, by default, only personal data which are necessary for each specific purpose of the processing were processed. In addition, the default settings used by TTL failed to ensure that personal data were not made accessible to third parties.

319. TTL's infringements of Article 25(1) GDPR affected each of those data subjects who were under the age of 18 because the appropriate technical and organisational measures that TTL failed to implement ought to have been in place in order to protect the rights and freedoms of each of those data subjects.

[327] Response to the PDD at [9.12]-[9.17].

320. TTL's infringements of Articles 5(1)(f) and 25(1) GDPR affected those who had sought to avail of the 'Family Pairing' setting as a means of strengthening rather than loosening the control of personal data of Child Users, and safeguarding such vulnerable user rights.

321. I find that TTL's infringements of Article 25(1) GDPR affected a large volume of data subjects because the appropriate technical and organisational measures that TTL failed to implement ought to have been in place in order to protect the rights and freedoms of each data subject from the start of the Relevant Period. The failure to implement the necessary safeguards in an effective manner at the appropriate time led to the possibility that Child Users could be targeted by bad actors for a variety of purposes, as set out above in relation to the risks of varying likelihood and severity. As noted earlier in this Decision, the personal data at issue related to a particularly vulnerable cohort of data subjects – children. The number of data subjects affected by TTL's infringements of Articles 25(1) and (2) GDPR is likely to be significant, in light of the numbers of Child Users that TTL had during the Relevant Period.

322. In assessing the level of damage suffered by the data subjects, I have had regard to the loss of control suffered by them over their personal data. A core element of the principle of data protection by default, Article 25(2) GDPR requires data controllers to ensure that they only process personal data that are necessary for each specific purpose. Data subjects are denied control over their personal data where their personal data is processed in a manner that is not necessary in relation the purposes of the processing.

323. I find that TTL's infringements of Articles 5(1)(c) and 25(2) GDPR prevented Child Users from exercising control over their personal data. The public-by-default processing constituted the processing of those users' personal data in a manner that went beyond what was necessary in relation to the purposes of the processing. This intrinsically denied those data subjects control over their personal data by extending the scope of processing beyond what was necessary in relation to the purposes. Such public-by-default processing placed these Child Users at risk of a variety of risks from bad actors, such as sexual exploitation, online harassment, grooming, and bullying. Therefore, I find that this loss of control represents a significant amount of damage to the data subjects.

324. I do not agree with TTL that Article 83(2)(a) GDPR only refers to "actual damage". This ignores the actual wording of Article 83(2)(a) which states:

> *"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"* (emphasis added)

325. Article 83(2)(a) GDPR requires that due regard must be given to the level of damage suffered by data subjects. The Article 29 Working Party's *'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679'* ("the **Fining Guidelines**") make clear that the imposition of a fine is not dependent on first establishing the precise level of damage that occurred, as follows:

> *"If damages have been* ***or are likely to be suffered*** *due to the infringement of the Regulation then the supervisory authority should take this into account in its choice of corrective measure, although the supervisory authority itself is not competent to award the specific compensation for the damage suffered. The imposition of a fine is not dependent on the ability of the supervisory authority to establish a causal link between the breach and the material loss* [...]"[328] (emphasis added)

[328] The Fining Guidelines at 11.

326. In assessing the level of damage for the purpose of Article 83(2)(a) GDPR, it is therefore appropriate that I have regard to the likely level of damage suffered by data subjects (including non-material damage) and to the overall number of data subjects who were affected by the infringements. The level of actual damage is a part – but not a prerequisite – of Article 83(2)(a) GDPR. Indeed, to interpret it otherwise would significantly diminish the effectiveness, proportionality and dissuasiveness of an administrative fine.

The nature of the infringements

327. The nature of both of TTL's infringements of Articles 12(1) and 13(1)(e) GDPR concern data subjects' right to information about the public-by-default processing. Article 12(1) GDPR sets out the manner in which controllers must communicate the information referred to in Articles 13 and 14 GDPR to data subjects. If controllers do not communicate that information in a manner that complies with Article 12(1) GDPR, data subjects may be denied an understanding of how their personal data is processed. It follows that these infringements of Article 12(1) GDPR concern data subjects' right to information. This is a cornerstone of the rights of the data subject. The provision of information in a *"concise, transparent, intelligible and easily accessible form, using clear and plain language"* goes to the very heart of the fundamental right of the individual to protection of their personal data, which stems from the free will and autonomy of the individual to share his/her personal data in a voluntary situation such as this. Article 12(1) GDPR emphasises the importance of the requirements *"in particular for any information addressed specifically to a child"*. Where an infringement of Article 12(1) GDPR concerns information provided to children, that infringement is even more likely to deny those data subjects an understanding of the processing and the risks associated with it.

328. Articles 83(4) and (5) GDPR are directed to the maximum fine that may be imposed in a particular case. The maximum fine prescribed by Article 83(5) GDPR is twice that prescribed by Article 83(4) GDPR. The infringements covered by Article 83(5) GDPR include infringements of the data subject's rights pursuant to Articles 12 to 22 GDPR and infringements of the principles in Article 5 GDPR. It is therefore clear that the legislator considered the data subject rights and the data protection principles in Article 5 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.

329. With regard to the nature of the infringements, TTL has submitted "*that information about the sharing of their personal data was provided to younger Users through various media and at various intervals, and that this ought to have an impact on the DPC's categorisation of seriousness of the infringements*" and "*As is clear from the matters set out above, TikTok does not agree with the manner in which the DPC has categorised the processing as "unauthorised or unlawful" or that it did not ensure appropriate security of the data. The ability for a Friend to message a younger User until mid-November 2020 of the Relevant Period, had a guardian enabled this, did not lessen the security of the younger User's data, nor have any impact on their data. When the factual evidence before the DPC is taken into account, TikTok submits that there is no basis to categorise these alleged infringements as serious in nature.*"[329]

330. I have also assessed the nature of TTL's infringements of Articles 12(1) and 13(1)(e) GDPR, regarding the public-by-default processing in light of the nature and scope of this processing. The nature of this processing concerns the publication of children's social media content on TikTok publicly by default. The scope concerns that publication to an indefinite and unrestricted audience. TTL's infringements of Articles 12(1) and 13(1)(e) GDPR likely denied children an

[329] Response to the PDD at [9.18]-[9.19]

understanding of this nature and scope. Accordingly, this lack of transparency likely affected children's decisions when registering for user accounts. It also likely affected their decisions on the personal data that they shared on their accounts after registering. I find that the nature of this infringement of Articles 12(1) GDPR is most serious in nature.

331. Article 83(4)(a) GDPR is directed to the maximum fine that may be imposed in a particular case that involves infringement of *"the obligations of the controller and processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43"*.

332. The nature of TTL's infringements of Articles 5(1)(f) and 25(1) GDPR concern its failure to implement appropriate measures designed to implement the data protection principles in an effective manner; and to integrate the necessary safeguards. Having regard to the nature and scope of the data processing, I consider that this failure to implement appropriate measures by design to be serious given, in particular, that it affected Child Users.

333. The nature of TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR concern its failure to ensure, using appropriate technical and organisational measures, that its processing of personal data was limited to what was necessary in relation to the purposes of that processing and the failure to ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. TTL's processing resulted in users' personal data being publicly available to an indefinite and unrestricted global audience. In light of the scope of the potential audience, I find that the nature of the infringement is serious.

The gravity of the infringements

334. In its Response to the PDD, TTL states that *"The DPC assesses the gravity of the infringements by reference to the number of data subjects and the level of damage suffered by them and how the alleged infringements somehow increased risks for data subjects. While TikTok of course acknowledges such risks for children, they are distinct from the processing and the two should not be conflated."*

335. In assessing the gravity of the infringements, I have had regard to the number of data subjects affected and the level of damage suffered by them. I have also had regard to how the infringements increased the risks posed by the processing to the rights and freedoms of TikTok users. These risks include, [redacted]physical harm to Child Users; online grooming or other sexual exploitation of Child Users and normalisation of sexual comments directed at/to Child Users; risk of social anxiety, self-esteem issues, bullying or peer pressure in relation to Child Users (in particular arising from public availability of content); risk of Child Users having access to harmful or inappropriate content; and risk of Child Users losing autonomy or rights (including control over data), as well as processing of personal data of vulnerable natural persons, that is children, and where such children are below the age of 13, the processing of their data, and high numbers of affected and potential affected Users. I find that the manner in which TTL's infringements increased the risks posed to TikTok users is highly relevant when assessing the gravity of the infringements.

336. In assessing the gravity of TTL's infringements of Articles 12(1) and 13(1)(e) GDPR regarding the public-by-default processing, I have had regard to how the infringement affected approximately [redacted] children. I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those children from exercising control over their personal data. Finally, I have also had regard to how the infringement increased the risks posed by the public-by-default processing to the rights and freedoms of the data subjects. In ordinary circumstances, children may be less aware of the risks, consequences and safeguards in relation

to the processing of their personal data. However, TTL's infringements of Articles 12(1) and 13(1)(e) GDPR significantly increased the likelihood that children would not understand the difference between public and private accounts. TTL's infringement also increased the likelihood that children would not understand that their accounts were set to public by default. This meant that Child Users were less likely to make informed decisions on the content of their public posts, for example, when deciding whether to share personal data that may be sensitive, such as location data. By denying children information in a clear and transparent form, these children were less likely to understand the risks of the public-by-default processing. Therefore, they were less likely to understand that there was a risk of contact from strangers and were less likely to take steps to mitigate against that risk. These infringements of Articles 12(1) and 13(1)(e) GDPR increased the risks posed by the public-by-default processing to the rights and freedoms of the Child Users. I find that the gravity of this infringement is highly serious.

337. I have assessed the gravity of TTL's infringement of Articles 5(1)(f) and 25(1) GDPR in light of how it resulted in TTL's failure to identify and to implement appropriate measures in respect of the processing to ensure compliance with the GDPR by design and to protect the rights of the data subjects. By failing to implement appropriate measures, TTL increased the risk posed by the processing to the rights and freedoms of those data subjects. I find that the gravity of TTL's infringement of Article 25(1) GDPR is serious.

338. In assessing the gravity of TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR regarding the processing, I have had regard to how TTL set the accounts of its users to public, by default. Therefore, the infringement affected a large number of Child Users, as set out above - the approximate total average number of registered EU TikTok users under the age of 18 was [redacted] I have also had regard to the direct damage suffered by the data subjects, specifically how the infringement prevented those users from exercising control over their personal data. The infringement also increased the risk posed to the rights and freedoms of those data subjects. The manner of processing due to the default settings resulted in users' accounts being made available to an indefinite and unrestricted global audience. In those circumstances, I find that the gravity of TTL's failure to ensure that its processing of personal data was limited to what is necessary in relation to the purpose of the processing is serious.

The duration of the infringements

339. The duration of TTL's infringements of Articles 12(1) and 13(1)(e) GDPR regarding the public-by-default processing commenced from the beginning of the Relevant Period on 31 July 2020. This continued until the end of the Relevant Period. For the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that this infringement under Article 12(1) GDPR lasted at least from 31 July 2020 until the end of the Relevant Period on 31 December 2020.

340. The duration of TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR regarding the processing commenced at the beginning of the Relevant Period. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement under the GDPR lasted at least from 31 July 2020 until the end of the Relevant Period of 31 December 2020.

341. The duration of TTL's infringements of Articles 5(1)(f) and 25(1) GDPR regarding the processing commenced at the beginning of the Relevant Period. The infringement was ongoing during the period of the Relevant Period. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement under the GDPR lasted at least from 31 July 2020 until the end of the Relevant Period of 31 December 2020.

342. I note that, prior to 25 October 2020, for under-16 users the download setting of videos on public accounts was set to 'off' but could be turned 'on' and from 25 October 2020, in Ireland, Italy and the Netherlands, TTL enabled restrictions which precluded the download of under-16 users' videos entirely. From January 2021, the download setting was set to 'off' for users aged 16-17.[330] Such restrictions took effect from January 2021 in all other EU countries where that feature was in operation. Further, from October 2020, Child Users only received account recommendations for other Child Users and their accounts were not recommended to users aged above 18. I note too that following the Relevant Period, TTL has made a number of changes from January 2021.[331]

M.2 Article 83(2)(b) GDPR: the intentional or negligent character of the infringement

343. In assessing the character of the infringements, I note that the GDPR does not identify the factors that need to be present in order for an infringement to be classified as either *'intentional'* or *'negligent'*. The Fining Guidelines provide that:

> *"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law".*[332]

344. The Fining 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".*[333]

345. In determining whether an infringement was intentional, I 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.

346. In determining whether an infringement was negligent, I 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.

347. TTL, in its Response to the PDD, makes a number of submissions:

> *"As a preliminary point, the PDD appears to proceed on the premise that all infringements are, by default, negligent if they are not found to be intentional. This is evident from the fact that the PDD provides only a cursory analysis of this issue before making Preliminary Findings. TikTok respectfully submits that this approach to characterising infringements is erroneous; it is clearly the case that infringements can arise despite the good faith efforts of a controller and can be inadvertent.*
>
> [...]

---

[330] Response to the Notice of Commencement at [10.19] and Images 12 and 13, and Response dated 21 February 2022 at 7. This initially referred to being in effect from 25 October 2020, per Footnote 197 of the Response to the PDD, this was clarified as being from January 2021 in fact.
[331] Submissions dated 14 April 2022 at [76].
[332] The Fining Guidelines at 11.
[333] The Fining Guidelines at 12.

TikTok does not consider there is any basis to consider that the alleged infringement of Articles 5(1)(c) and 25(1) and (2) was intentional. This requires a very high standard to be met; the DPC is required to "demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement". In short, TikTok must have known and willingly taken steps it knew would infringe the GDPR for any infringement to be intentional. It is submitted that the PDD does not disclose any factual or evidential basis for this Preliminary Finding.

[...]

TikTok welcomes the acknowledgement that TikTok did not act intentionally to infringe the GDPR in respect of Articles 5(1)(f) and 25(1) GDPR. However, it respectfully suggests that the PDD does not provide any basis for a conclusion TikTok was negligent. This Preliminary Finding appears to be based on the fact that TikTok "ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) and 25(1) given that the 'Family Pairing' setting more generally allowed the non-Child User to tighten privacy controls but for reasons that remain unclear allowed the non-Child User to enable Direct Messages for over-16s, a means of direct communication with the Child user." However, this fails to have regard to the various limitations and safeguards TikTok put in place regarding direct messages (such as the restriction for Users under 16, and that direct messages could only be sent to and from "Friends" and the verification steps required to ensure that only guardians were able to enable to feature) to ensure that it was compliant with Articles 5(1)(f) and 25(1) GDPR. These measures are set out in sections 5.125 - 5.136 above. While the DPC may disagree with the approach adopted by TikTok, it cannot be said that there was a failure on the part of TikTok akin to those identified by the WP29.

[...]

TikTok welcomes the acknowledgement that it did not act intentionally to infringe the GDPR in respect of Articles 12(1) and 13(1)(e) GDPR. However, it respectfully suggests there are no grounds for the proposed finding that TikTok was negligent. This Preliminary Finding appears to be premised on the fact that there is an "initial layer of information and that there is a prescriptive requirement to provide explicit information on certain specific purposes of processing in this layer. TikTok disagrees that there is any such requirement in the GDPR - a point the DPC appears to concede elsewhere in the PDD.162 The prescriptive approach of the DPC is inconsistent with Article 12 GDPR and the discretion afforded to controllers".[334]

348. TTL's infringements of Articles 12(1) and 13(1)(e) GDPR regarding the public-by-default processing concerns its failure to provide information concerning the purposes of this processing in a clear and transparent form. Hence, the characteristics of this infringement concern the lack of clarity and transparency in the information provided. In order to classify this infringement as intentional, I must be satisfied that (i) TTL wilfully presented the information in the manner outlined and (ii) that it knew at the time that the information was not presented in a clear and transparent form. In making this determination, I must rely on objective elements of TTL's conduct that show the presence or absence of wilfulness and knowledge. While TTL wilfully decided on the content of its registration stage and Privacy Policy, objective elements of TTL's conduct at the time suggest that this infringement was not intentional. At the Relevant

[334] Response to the PDD at [9.27]-[9.33].

Period, a number of TikTok's in-app platform information areas and ancillary sources such as the TikTok Help Centre and the TikTok Safety Centre provided information that the accounts were public-by-default and information on how to switch. These sources were accessible via both the app and the website; however, they were not hyperlinked in the Privacy Policy. This objectively suggests that TTL intended to provide this information with clarity and transparency and did not intend to deny Child Users an understanding of the purposes of the processing, but rather unintentionally fell short of the standard required by presenting the information without the required clarity and transparency. Therefore, I find that this infringement was not intentional.

349. However, I find that TTL's infringements of Articles 12(1) and 13(1)(e) GDPR regarding the public-by-default processing was negligent in the particular circumstances. Articles 12(1) and 13(1)(e) GDPR do not prescribe standard formats or practical arrangements when providing information. However, TTL ought to have been aware of how this obligation in the circumstances necessitated information on the purposes of processing in the initial layer of information. TTL also ought to have been aware of the requirement for the Privacy Policy to provide explicit information on the specific purposes of the processing. In making this finding, I have had particular regard to how a company the size of TTL ought to have been aware of its precise transparency obligations, in particular, in light of the quantity of children's data processed on the platform. I have also had regard to how the nature of TTL's business entails the processing of large volumes of personal data. Therefore, I am satisfied that TTL was negligent within the meaning of Article 83(2)(b) GDPR.

350. TTL's infringement of Articles 5(1)(f) and 25(1) GDPR concerns its failure to implement appropriate measures to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing. Hence, the characteristics of this infringement concerns that lack of appropriate technical and organisational measures for the duration of the infringement. In order to classify these infringements as intentional, I must be satisfied that (i) TTL wilfully omitted to implement appropriate technical and organisational measures and (ii) that it knew at the time that the measures that it implemented were not sufficient to meet the standards required by Articles 5(1)(f) and 25(1) GDPR. Having considered the objective elements of TTL's conduct, as set out above, I do not consider that TTL wilfully omitted to implement appropriate measures. While TTL's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) and 25(1) GDPR, I do not consider that this failure was wilful on TTL's part. However, it is clear that TTL ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) and 25(1) GDPR given that the 'Family Pairing' setting more generally allowed the non-Child User to tighten privacy controls but, for reasons that remain unclear, allowed the non-Child User to enable direct messages for over-16s, a means of direct communication with the Child User. I find that TTL's failure to implement appropriate measures pursuant to Articles 5(1)(f) and 25(1) GDPR in respect of its processing was negligent in the circumstances.

351. TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR concerns its failure to ensure, using appropriate technical and organisational measures, that its processing of personal data was limited to what was necessary in relation to the purposes of the processing. Hence, the characteristics of this infringement concern TTL's failure to implement appropriate measures to ensure that Child Users' personal data was not made accessible (without the user's intervention) to an indefinite number of natural persons by default. In order to classify these infringements as intentional, I must be satisfied that (i) TTL wilfully set the platform settings for users regarding the relevant features to public-by-default, and (ii) that it knew at the time that this would result in personal data processing that was not limited to what was necessary in relation to the purposes. In making this determination, I must rely on objective elements of

TTL's conduct that show the presence or absence of wilfulness and knowledge. I find that TTL wilfully decided to set all Child User accounts as public-by-default. I find that TTL knew that this would result in personal data processing that was not limited to what was necessary in relation to the purposes, particularly as TTL stated *"that, by design, TikTok is a platform which is designed to enable users to share video content that they create. Younger Users may therefore have specific and legitimate reasons to want to have a public account, such as where they are seeking to build a wider following for their content."*[335] Therefore, TTL's infringements of Articles 5(1)(c) and 25(1) and (2) GDPR regarding the public-by-default processing was intentional.

352. I do not accept the submissions by TTL, set out above. There is a distinction of terms between internationality of action and that of infringement. TTL could have made various choices with regard to its processing and did not do so, and indeed, its actions demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration, as set out above in detail.

M.3 Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects

353. This Decision outlines the measures that TTL put in place from October 2020, as well as the changes following the Relevant Period.[336] TTL submits that more than "limited mitigation" should be afforded to it for these changes.[337] Such measures indeed appear to directly mitigate the issues set out, following the Relevant Period. However, it is not always possible to retrospectively correct a past lack of control, as personal data has already been published and data subjects may already have suffered consequential damage as a result.

354. I note that the above actions by TTL may have reduced the probability of further additional risk of damage to data subjects after the infringements occurred for the purpose of Article 83(2)(c) GDPR. Having regard to these actions for the purpose Article 83(2)(c) GDPR, I am of the view that the actions provided limited mitigation of the damage to data subjects, and accordingly I consider that the actions are of mitigating value.

M.4 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

355. The Fining 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".*[338]

356. I have found that TTL infringed Articles 25(1) and 25(2) GDPR regarding its processing of personal data. I consider that TTL holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. It is clear that TTL did not do *"what it could be expected to do"* in the circumstances assessed in this Decision. However, in circumstances where this factor forms the basis for the finding of the infringements of Article 25 GDPR against TTL, this factor cannot be considered aggravating in respect of the infringements. Rather, I must

[335] Response to the Notice of Commencement at [10.2], see also Submissions dated 14 April 2022 at [63].
[336] Submissions dated 14 April 2022 at [76] and [128].
[337] Response to the PDD at [9.35].
[338] The Fining Guidelines at 13.

independently consider, pursuant to Article 83 GDPR, whether these infringements of Article 25 GDPR merit the imposition of administrative fines in and of themselves.

357. In its Response to the PDD, TTL states that the basis for considering that it: "*holds a high degree of responsibility for this failure*" or why "*it is clear that TTL did not do "what it could be expected to do" in the circumstances*" has not been articulated.[339] I do not accept this. It is set out in detail above with respect to the various findings. In any event, as I have stated, this factor cannot be considered aggravating in respect of the infringements.

M.5 Article 83(2)(e): any relevant previous infringements by the controller or processor

358. No relevant previous infringements arise for consideration in this context.

359. TTL submits this should be considered mitigatory. I do not agree, rather that there are no relevant previous infringements does not constitute an aggravating factor.[340]

M.6 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

360. Throughout the Inquiry, TTL has maintained that it did not infringe the GDPR in respect of the matters under consideration. Nonetheless, it has made significant changes to the public-by-default processing. TTL's motivation for these changes was not to remedy the infringements because TTL's position throughout the inquiry is that it has not infringed the relevant provisions. Regardless of the motivation for the changes, I consider that TTL is entitled to mitigation for this action because it contributes towards remedying the infringements. These actions include:

> *Private Accounts*
> *(A) From January 2021, under 16 Users were no longer required to make the choice during the account registration process to choose a private account or skip the private account option. Instead, these younger Users' accounts are defaulted to private, without any ability for these younger Users to choose a public account during the registration process. These younger Users are informed through a pop-up notification during the registration process that their account has been set to private (so that only approved Users can view their videos) and that they can review and manage their account through their app settings.*
>
> *Duets and Stitches*
> *(B) From January 2021, the Duet and Stitch feature was disabled for all under 16 Users, meaning that other Users cannot Duet or Stitch with videos created by under 16 Users. By default, only "Friends" of Users aged 16 or 17 can make Duets and Stitches of videos created by these Users.*
>
> *Video Comments*
> *(C) From January 2021, under 16 Users do not have the option of allowing their videos to be commented on by "Everyone" and can only choose to receive comments from "Friends" or "No One".*
>
> *Downloading Videos*

[339] Response to the PDD at [9.36].
[340] Response to the PDD at [9.38]

(D) From January 2021, for younger Users aged 16 or 17, the download feature was turned "off" by default.

Suggest Your Account to Others
(E) From January 2021, this setting is turned off for under 16 Users by default.[341]

361. While I consider that this action is mitigating because it contributes towards remedying the infringements, I make this finding without prejudice to the question of whether TTL's on-going processing complies with the GDPR.

M.7 Article 83(2)(g): the categories of personal data affected by the infringement

362. The categories of personal data affected by TTL's infringements of Articles 12(1), 13(1)(e) 5(1)(c), 25(2), 5(1)(f) and 25(1) GDPR, regarding the public-by-default processing reflect the categories of personal data likely shared by children on public-by-default accounts. By setting children's accounts to public by default, TTL determined that the content of those accounts would be visible to an indefinite and unrestricted global audience. Therefore, it follows that TTL's infringements affected any categories of personal data likely shared on those public-by-default accounts.

363. It is not practicable for the purposes of this Inquiry to analyse the specific personal data actually shared by children on their public-by-default accounts. The TikTok platform primarily allows users to share their personal data through video clips, and including through public comments and conversations. TTL's infringements of Articles 12(1) and 13(1)(e) GDPR risked denying children an understanding that their social media content would be visible to an indefinite and unrestricted audience. This, in turn, likely affected the categories of personal data that those children decided to share on those accounts, including categories of personal data intended for a more restricted audience of followers. In all the circumstances, I am satisfied that the categories of personal data likely shared by children on their public-by-default accounts include an extensive range of categories. This personal data shared is likely to include information on users' daily lives and interests. The personal data may be sensitive as it may make a Child User identifiable to dangerous persons due to the public processing of that personal data.

364. TTL submits that:

> *"TikTok does not consider it appropriate that the DPC appears to have relied on assertions that "sensitive" personal data has been impacted by the processing as an aggravating factor without conducting any analysis as to whether this is in fact the case, and absent any evidence that this has occurred. As with the DPC's position on alleged damage suffered by younger Users, this is based on speculation and hypothetical risks. This proposed finding is entirely speculative and this approach is not appropriate, particularly in circumstances where fines of the magnitude proposed may be imposed on TikTok.*
>
> *In any event, TikTok submits that this factor should be considered less relevant in circumstances where the categories of personal data affected have been processed as a direct result of the actions and choices made by younger Users. This can be*

[341] Submissions dated 14 April 2022 at [76]. Per [34] and Footnote 37 of the Submissions dated 14 April 2022, TTL states it disabled downloads for new and existing under-16 users in Ireland, Italy, and the Netherlands in October 2020. In January 2021, TTL disabled downloads for new and existing users in the remaining EU countries where that feature was in operation.

contrasted with a scenario where, due to a personal data breach, sensitive data is inadvertently disclosed to unauthorised third parties. Younger Users remained in control of their accounts at all times, as explained in this Response."[342]

365. I do not agree with this in circumstances where I have not accepted the premise of this submission with regard to public-by-default processing, nor that there must be actual damage.

M.8 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

366. The infringements became known to the DPC as a result of contact received from the organisations discussed in Section C.1 of this Decision.

367. TTL engaged fully with the DPC from the Notice of Commencement.

368. TTL submits this should be considered mitigatory. I do not agree, rather that there was no failure to engage does not constitute an aggravating factor.[343]

M.9 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

369. Corrective powers have not previously been ordered against TTL with regard to the subject matter of this Decision.

370. TTL submits this should be considered mitigatory. I do not agree, rather that there are no previous corrective powers ordered does not constitute an aggravating factor.[344]

M.10 Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

371. Such considerations do not arise in this case.

M.11 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

372. I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the particular circumstances of the case.

M.12 Decision on Administrative Fine

373. In deciding whether to impose an administrative fine in respect of each infringement, I have had regard to the factors outlined in Article 83(2)(a) – (k) GDPR cumulatively, as set out above. However, I have considered each distinct infringement separately when applying those factors, when deciding whether to impose an administrative fine, and when deciding the amount of

[342] Response to the PDD at [9.40]-[9.41].
[343] Response to the PDD at [99.42].
[344] Response to the PDD at [9.43].

each administrative fine. I have also had regard to the effect of the order and reprimand in ensuring compliance with the GDPR. The order will assist in ensuring compliance by mandating specific action on the part of TTL in order to re-establish compliance with specific findings of infringements. The reprimand will contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements. However, I consider that these measures alone are not sufficient in the circumstances to ensure compliance. I find that administrative fines in respect of each of the infringements are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

374. 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, a reprimand 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) GDPR 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, reprimands 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."*

375. While the order made pursuant to this Decision will re-establish compliance with the specific infringements identified, I do not consider this measure appropriate to deter other future serious infringements. While the reprimand will assist in dissuading TTL and other entities from similar future non-compliance, in light of the seriousness of the infringements, I do not consider that the reprimand is proportionate or effective to achieve this end. I find that administrative fines are necessary in respect of each of the infringements to deter other future serious non-compliance on the part of TTL and other controllers or processors carrying out similar processing operations concerning children's data. The reasons for this finding include:

    a. First, the processing at issue – both in relation to platform settings and to age verification disclose high and severe risks in relation to Child Users and to children under the age of 13.

    b. In relation to public-by-default processing, where a Child User were to avail of the relevant public features of the TikTok platform they could lead in the first instance to Child Users losing autonomy and control over their data, and, in turn, they could become targets for bad actors, given the public nature of their use of the TikTok platform. This could also lead to a wide range of potentially deleterious activities, including online exploitation or grooming, or further physical, material or non-material damage where a Child User inherently or advertently reveals identifying personal data. There is the identified risk of social anxiety, self-esteem issues, bullying or peer pressure in relation to Child Users. Insofar as this Inquiry relates to age verification platform settings, where a child under the age of 13 were to gain access to the TikTok platform, further to the risks identified in relation to

public-by-default processing which apply equally, if not more severely to children under 13, such as a child under 13 may be at risk of viewing and accessing materials that are harmful or inappropriate for a child of such youth, particularly given that the TikTok platform is not intended for children under 13.

c. As well as this, generally, I also note that the processing which is at issue in this Inquiry involves the public and off-TikTok dissemination of the personal data of Child Users. This presents a severe risk for Child Users.

d. Further to these identified risks, it is also clear that TTL's processing of users' personal data presented risks relevant to a number of the data protection principles provided for under Article 5 GDPR, such as under Articles 5(1)(b), 5(1)(c), and 5(1)(f) GDPR.

e. Second, TTL implemented a default account setting for Child Users which allowed anyone (on or off TikTok) to view social media content posted by Child Users. In particular, this processing was performed to a global extent, and in circumstances where TTL did not implement measures to ensure that by default the social media content of Child Users was not made accessible (without the user's intervention) to an indefinite number of natural persons. Such processing was contrary to Articles 25(1) and 25(2) GDPR, and Article 5(1)(c) GDPR.

f. Third, 'Family Pairing' allowed a non-Child User to enable direct messages for Child Users above the age of 16. This processing does not ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and is not an appropriate technical and organisational measure designed to implement the integrity and confidentiality principle in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects, contrary to Articles 5(1)(f) and 25(1) GDPR.

g. Fourth, TTL did not provide Child Users with information on the categories of recipients or categories of recipients of personal data using clear and precise language, and did not provide Child Users with information on the scope and consequences of the public-by-default processing (that is, operating a social media network which, by default, allows the social media posts of Child Users to be seen by anyone) in a clear and transparent form, in particular insofar as the information provided did not make it clear that this would occur, contrary to Articles 13(1)(e) and 12(1) GDPR.

376. Based on the analysis I have set out, I will impose the following administrative fines:

(a) In respect of TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR **(Finding 1)**, a fine of between €55 million and €100 million.

(b) In respect of TTL's infringement of Articles 5(1)(f) and 25(1) GDPR **(Finding 3)**, a fine of between €55 million and €100 million.

(c) In respect of TTL's infringements of Articles 12(1) and 13(1)(e) GDPR **(Finding 5)**, a fine of between €110 and €180 million.

377. I have taken into account – in accordance with the approach of the EDPB – the total worldwide annual turnover of the undertaking of which TTL forms part, namely the group of companies headed by ByteDance Ltd, as set out below, in my calculation of the appropriate amount of the administrative fines. I consider that it is appropriate to do so in order to ensure that the administrative fines satisfy the requirement in Article 83(1) GDPR for any administrative fine imposed to be effective, proportionate and dissuasive in each individual case.

378. In its Response to the PDD, TTL stated:

> [I]*nsofar as the DPC has had regard to turnover in calculating the administrative fines proposed in accordance with Articles 83(1) and (2) – whether of TikTok or ByteDance Ltd – in calculating the administrative fines, as opposed to the applicable fining caps, this is an error of law. This approach is not provided for in either Articles 83(1) or 83(2), and constitutes a clear breach of Article 83(2). TikTok respectfully submits, therefore, that were the DPC to maintain this approach, this will constitute a clear error of law.*[345]

379. I do not accept TTL's submission in this regard. The EDPB determined in its Binding Decision 1/2021 that: [346]

> *…the EDPB takes the view that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR.*[347]

380. In having determined the quantum of the fines above, I have taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be *"effective, proportionate and dissuasive"* in each individual case. My view is that, in order for any fine to be *"effective"*, it must reflect the circumstances of the individual case. As outlined above, the infringements are all serious in nature and in gravity. The infringements concern personal data belonging to children and the infringements all increased the risks posed by the processing to the rights and freedoms of those children.

381. In order for a fine to be *"dissuasive"* it must dissuade both the controller/processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. I consider that the fining ranges set out above are dissuasive for both. I am further satisfied that the fines are no greater than required to achieve deterrent effect, noting the industry in which TTL operates, and the extent of internal and external resources available to it.

382. As regards the requirement for any fine to be *"proportionate"*, this requires me to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fines above do not exceed what is necessary to enforce compliance with the GDPR taking into account the size of TTL's user base, the loss of control over personal data suffered by the data subjects, and how infringements increased the risks posed by the processing to the right and freedoms of the data subjects.

---

[345] Response to the PDD at [9.49].
[346] EDPB 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
[347] *Ibid.* at [412].

383. TTL submits that there is an "over-focus" on dissuasion and that the PDD fails to explain how fines of the magnitude proposed are the least onerous measure available to achieve the DPC's objective in circumstances where TTL has already voluntarily implemented changes to address the relevant issues and to mitigate any theoretical risks they may have posed to data subjects. TTL also states that I have proceeded to set out the analysis on the infringements largely in a broad-brush manner that is not compatible with Article 83(2) GDPR and the duty to give reasons, which has made it extremely difficult for TTL to make meaningful submissions.[348]

384. I do not accept this. First, I have considered in detail all of the factors under Article 83(1) GDPR which I have addressed in detail. This is similarly the case with regard to the factors under Article 83(2)(a)-(k) GDPR. Extensive reasoning and engagement has been provided in relation to all aspects of these criteria. It is simply not sustainable or factually borne out to suggest that insufficient reasoning has been provided or that it was "impossible" to understand how the administrative fines have been calculated. Indeed, in its Response to the PDD, despite its claim, TTL has somehow managed to make very detailed, nuanced and lengthy submissions with regard to all factors, which have been fully considered.

385. I am satisfied that the fines specified would, if imposed on TTL, be effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

M.13 Article 83(3) GDPR

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

387. 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.*

388. I note that, by way of EDPB Binding Decision 01/2021, the EDPB recorded its assessment of the meaning and effect of Article 83(3) GDPR. In light of the binding nature of that decision and the DPC's obligations of cooperation and consistency in, inter alia, Articles 60(1) and 63 GDPR, it is necessary for me to follow the EDPB's interpretation of Article 83(3) GDPR.[349]

389. The relevant passage of EDPB Binding Decision 01/2021 is as follows:

> *315. All CSAs argued in their respective objections that not taking into account infringements other than the "gravest infringement" is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the*

[348] Response to the PDD at [9.7]-[9.10].

[349] European Data Protection Board, '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' (28 July 2021) accessible via https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.

316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.

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

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

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

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

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

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

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

infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.

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

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

326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.

327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness.

390. The impact of this interpretation is that administrative fine(s) should be imposed cumulatively, as opposed to imposing only the fine that corresponds to the gravest infringement. The only applicable limit for the total fine imposed, by reference to this interpretation, is the overall fining "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.

391. TTL submits, in its Response to the PDD, that:

TikTok considers that the DPC has incorrectly interpreted and applied Article 83(3) GDPR in the PDD. There is no justification for the imposition of cumulative

administrative fines in this Inquiry in the manner proposed in the PDD - especially where doing so results in administrative fines which are disproportionate and, as such, incompatible with Article 83(1) GDPR.

[...]

The DPC is required to ensure, in accordance with Article 83(1) GDPR, that any proposed administrative fine is proportionate. TikTok respectfully submits that any decision which purports to impose multiple sanctions for the same conduct (i.e. the same or linked processing operations) must necessarily be deemed to be disproportionate and, therefore, contrary to Article 83(1) and to the fundamental principle of proportionality under EU law, as enshrined in Article 49 of the Charter of Fundamental Rights.

[...]

TikTok notes that the DPC justifies the approach adopted in the PDD by reference to Decision 1/2021. However, this decision is not binding on the DPC in this Inquiry and, in any event, is currently under appeal

[...]

TikTok submits that the DPC has misinterpreted Article 83(3) GDPR and has failed to have regard to the requirements of Articles 83(1) GDPR in the PDD by failing to acknowledge the overlapping nature of the alleged infringements, with the result that the cumulative amount of the administrative fines is disproportionate and excessive. TikTok respectfully requests the DPC take such considerations into account and that this - in and of itself - would warrant a substantial reduction in the total overall administrative fine being proposed.[350]

392. I do not accept these submissions. First, fines have been levied for individual infringements of the GDPR. Simply because they are related to the platform settings does not in itself mean that multiple sanctions are being imposed for the same conduct. Indeed, the detailed and individualised examination of the issues at length shows this. Second, I do not accept that there is either a misinterpretation of Article 83(3) GDPR nor that the fines are excessive or disproportionate – these issues have been dealt with in detail above.

393. I consider that TTL's infringement of Article 12(1) GDPR is the gravest infringement concerning the transparency of public-by-default settings. This is for the reasons as set out above. I further note that the associated maximum possible fine for that infringement under Article 83(5) GDPR is 4% of the total worldwide annual turnover of the undertaking of which TTL forms part, namely the group of companies headed by ByteDance Ltd. It is further to be noted that EDPB Binding Decision 01/2021, from which I quoted above, also directed the DPC to take account of the turnover of the relevant undertaking in the calculation of the fine amounts and I have factored that turnover figure into my calculations of the individual infringement fining ranges. When the ranges for the individual infringements are added together, a fining range with a maximum of €380 million arises. The combined fines are below 4% of the total worldwide annual turnover of the undertaking of which TTL forms part, namely the group of companies headed by ByteDance Ltd., as considered below.

[350] Response to the PDD at [9.50]-[9.57].

M.14 Articles 83(4) and (5) GDPR

394. Turning, finally, to Articles 83(4) and (5) GDPR, I note that these provisions operate to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

395. Article 83(4) GDPR provides as follows:

> *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> *(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;*
>
> *[…]*

396. Article 83(5) GDPR 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:*
>
> *(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;*
>
> *(b) the data subjects' rights pursuant to Articles 12 to 22;*
>
> *[…]*

397. 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 GDPR clarifies, in this regard, that:

> *Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.*

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

> *an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed*[351]

399. 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,

[351] Judgment of 23 April 1991, *Höfner and Elser v Macrotron GmbH*, C-41/90, EU:C:1991:161 at [21].

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.[352]

400. 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.

401. 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.[353]

402. 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.[354]

403. The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary.[355]

404. The General Court of the EU 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.[356] 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*

---

[352] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:536 at [58] – [60].
[353] Judgment of 14 September 2016, *Ori Martin and SLM v Commission*, C-490/15 P, ECLI:EU:C:2016:678 at [60].
[354] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:536.
[355] Judgment of 8 May 2013, *Eni v Commission*, C-508/11 P, EU:C:2013:289 at [48].
[356] Judgments of 7 June 2011, *Total and Elf Aquitaine v Commission*, T-206/06, EU:T:2011:250 at [56]; Judgment of 12 December 2014, *Repsol Lubricantes y Especialidades and Others v Commission*, T-562/08, EU:T:2014:1078 at [42]; and Judgment of 15 July 2015, *Socitrel and Companhia Previdente v Commission*, T-413/10 and T-414/10, EU:T:2015:500 at [204].

subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company …[357]

405. 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.

406. 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.

407. As noted above, per TTL's Director's Report and Financial Statement for year ending 31 December 2021, available from the Companies Registration office, TTL is a private company limited by shares, incorporated on 12 October 2018. TTL's sole shareholder is TikTok Information Technologies UK Limited. TTL 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 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. […] .*[358]

408. For the purposes of the PDD, it seemed to be, therefore, subject to the submissions of TTL in this regard should they wish to attempt to rebut the presumption of decisive influence, that the corporate structure of the entities concerned is such that ByteDance Ltd. is in a position to exercise decisive influence over TTL's behaviour on the market. Accordingly, a rebuttable presumption arose to the effect that ByteDance Ltd. does in fact exercise a decisive influence over the conduct of TTL on the market.

---

[357] Opinion of Advocate General Kokott in *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:262 at [73], as cited in Judgment of 12 July 2018, *Goldman Sachs Group, Inc. v European Commission*, T-419/14, ECLI:EU:T:2018:445 at [51].

[358] TTL, 'Director's Report and Financial Statement' (Year Ending 31 December 2021) at 11.

409. If this presumption is not rebutted, it would mean that ByteDance Ltd. and TTL constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant fining cap for the purpose of Articles 83(4) and (5) GDPR, would fall to be determined by reference to the combined turnover of TTL and ByteDance Ltd. As noted in the PDD, ByteDance Ltd. is incorporated and registered in the Cayman Islands and does not report its total revenue for each year.

410. TTL was invited to make submissions in this regard and in its Response to the PDD it did so.

411. First, TTL states that competition law principles do not apply in this context and does not accept that Recital 150 GDPR, "*a mere recital*" can be relied upon as creating a rule which is not otherwise provided for anywhere in the text of the GDPR.[359]

412. Second, TTL also submits that insofar as such principles and concepts are relevant that the DPC's reliance on the turnover of ByteDance Ltd., a separate legal entity, is based on a misapplication of such principles:

> *In circumstances where ByteDance Ltd is not alleged to have acted as a controller or a processor, and whether no entity other than TikTok has been found to have committed any infringement, having regard to the turnover of ByteDance Ltd or any other entity would void the separation of corporate liability provided for by the GDPR and as result violate the essence of the liability regime set forth in the GDPR.*[360]

413. Third, TTL also submits that EDPB Binding Decision 1/2021 is not binding and does not provide a basis for the DPC's approach with regard to turnover.[361] TTL also notes that:

> *In circumstances where the DPC has not sought to hold ByteDance Ltd. jointly and severally liable with TikTok, the fine in question, calculated based on ByteDance Ltd.'s purported global turnover as reported in unsubstantiated press reports, is not reflective of the financial capacity of TikTok. The DPC's reliance on ByteDance Ltd's purported global turnover is misplaced and results in a fine that far exceeds what is required to be effective and dissuasive.*[362]

414. Fifth, TTL states that there was a wrongful reliance on and application of the presumption of decisive influence in that:

> *The DPC relies entirely on the presumption of decisive influence to conclude that TikTok and ByteDance Ltd are part of a single undertaking. This presumption is based solely on the fact that TikTok's Director's Report and Financial Statement for year ending 31 December 2020 note that ByteDance Ltd. is TikTok's ultimate parent. From this fact alone, the PDD provisionally finds that "a rebuttable presumption arises to the effect that ByteDance Limited does in fact exercise a decisive influence over the conduct of TTL on the market". The PDD suggests that, if this presumption is not rebutted, this "would mean that ByteDance Ltd and TTL constitute a single economic unit and therefore for a single undertaking within the meaning of Article 101 TFEU". The DPC then concludes on this basis that the appropriate fine ought to be calculated by reference to the combined turnover of TikTok and ByteDance Ltd.*

[359] Response to the PDD at [9.65]-[9.71].
[360] Response to the PDD at [9.72]-[9.80].
[361] Response to the PDD at [9.81]-[9.84].
[362] Response to the PDD at [9.84].

This is not an adequate factual or evidential basis for purporting to rely on the presumption of decisive influence. Nor has any evidence been adduced showing that decisive influence was in fact exercised. As noted above, ByteDance Ltd is a holding company, incorporated in the Cayman Islands, which maintains interests in various different businesses around the world.

The provisions in the GDPR are based on certain defined concepts such as that of a controller, which is the legal entity responsible for complying with the rules provided for in GDPR. In considering whether ByteDance Ltd and TikTok constitute a single economic unit, therefore, the DPC ought to look at the processing of personal data and make an assessment of the relevant undertaking on that basis. In the context of the processing of personal data and the related decision making, which is the relevant behaviour that the DPC should assess for the purposes of its undertaking assessment, there is simply no basis to suggest that ByteDance Ltd exercised decisive influence over the processing of personal data by TikTok.[363]

415. I do not accept TTL's submissions in relation to the above for the following reasons:

i. Recital 150 GDPR expressly states that "[w]*here 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*." Recital 150 indicates an intention by the EU legislature to incorporate the definition of "*undertaking*" from EU competition law into the GDPR insofar as the term "*undertaking*" is used in connection with the imposition of administrative fines. This arises, in particular, in Articles 83(4) to (6) GDPR. TTL's interpretative arguments regarding Recital 150 are novel, to put it mildly, but ultimately unsustainable.

ii. The concept of an "undertaking" in Article 101 and 102 TFEU is not defined in the text of those articles, but rather has developed by interpretation in the case law of the EU courts in the field of EU competition law. The concept of "decisive influence" has been developed by the CJEU in that context for the purpose of determining whether one or more natural or legal persons constitute a single economic entity. It is not apparent from the text of the GDPR whether or how the concept of "decisive influence" is to be adapted or applied differently in the statutory context of the GDPR. In particular, it is not clearly indicated that the exercise of determining whether one entity exerts "decisive influence" over a another's conduct on the market is to be conflated with the question of which of the two entities takes decisions concerning data processing activities for the purposes of the GDPR. If it had been the intention of the EU legislature to align the definition of the relevant "undertaking" for the purposes of Article 83(4) to (6) GDPR with the definition of a "controller" within the meaning of Article 4(7) GDPR – that is, the "*natural or legal person* [...] *which, alone or jointly with others, determines the purposes and means of the processing of personal data*" – it would presumably have done so explicitly. As it stands, there is no clear basis in the text of the GDPR for TTL's contention that having "decisive influence" should be equated, in a GDPR context, with having responsibility as a controller for data processing activities and related decision-making about personal data.

iii. A presumption of decisive influence cannot be rebutted merely by showing that a subsidiary (acting as a controller within the meaning of Article 4(7) GDPR) makes its

[363] Response to the PDD at [9.85]-[9.87].

own decisions relating to the processing of personal data, independently of its parent company. In this connection, the General Court of the EU has acknowledged that "[o]*perational independence does not, in itself, prove that a subsidiary decides upon its conduct on the market independently of its parent company. The division of tasks between subsidiaries and their parent companies and, in particular, the fact that the local management of a wholly owned subsidiary is entrusted with operational management is normal practice in large undertakings composed of a multitude of subsidiaries ultimately owned by the same holding company.*"[364] The CJEU has emphasised that in examining whether the parent company is able to exercise decisive influence over the market conduct of its subsidiary, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to its parent company and, therefore, of economic reality.[365] The fact that a subsidiary enjoys autonomy in some aspects of its commercial activities is not sufficient, by itself, to overcome the rebuttable presumption of decisive influence which arises where a subsidiary is wholly owned (or almost wholly owned) by its parent company.[366] Rather, the key consideration is whether, in view of the economic, organisational and legal links between the parent and the subsidiary, the subsidiary enjoys real autonomy with respect to its conduct on the market overall.

iv. Accordingly, the fact that TTL acts as a controller within the meaning of Article 4(7) GDPR for the personal data of EU users of the TikTok platform does not mean that the presumption of decisive influence by its parent company, ByteDance Ltd, is necessarily rebutted.

v. TTL has not put forward any additional evidence in its submissions that would permit me to form a contrary view to that expressed above as to the exercise of decisive influence by ByteDance Ltd. over TTL's conduct on the market. TTL's Financial Statements for the financial year ending 31 December 2021 themselves confirm that ByteDance Ltd. is TTL's ultimate parent, and while TTL states there is no "*adequate factual or evidential basis for purporting to rely on the presumption of decisive influence*" and "*nor has any evidence been adduced showing that decisive influence was in fact exercised*", no probative evidence has been provided to the contrary.

416. I note that Articles 83(4) and (5) GDPR require the applicable fining "cap" to be determined by reference to the "*total worldwide annual turnover of the preceding financial year*". In circumstances where "preceding", in this regard, means the financial year preceding the year in which the relevant decision has been adopted, I sought updated financial information from TTL, shortly before the adoption of this Decision, in relation to the total worldwide annual turnover of the group of companies headed by ByteDance Ltd. for the financial year ending 31 December 2022. By way of the cover letter accompanying the Final Submissions, TTL confirmed that the estimated turnover for the group of companies headed by ByteDance Ltd. for the financial year ending 31 December 2022 was approximately [redacted]

417. Applying the above to Article 83(5) GDPR (which, for the reasons already explained above, provides the basis for the assessment of the applicable fining "cap"), I note that the maximum possible fine that might be imposed by this Decision (calculated by taking the notional maximum

[364] Judgment of 11 July 2019, *Huhtamäki Oyj,* T-530/15, EU:T:2019:498 at [228].
[365] Judgment of 11 July 2013, *Commission v. Stichting Administratiekantoor Portielje*, C-440/11 P, EU:C:2013:514 at [60] and [66].
[366] Judgment of the CJEU of 8 May 2013, *Eni v. Commission*, C-508/11, EU:C:2013:289 at [64]-[68].
[367] Letter from TTL to Data Protection Commission (25 August 2023) at [4.2.2].

figure permitted by each of the identified fining ranges, and adding them together) does not exceed the maximum limit of 4% of the total worldwide annual turnover for the financial year ending 31 December 2022 of the undertaking of which TTL forms part, namely the group of companies headed by ByteDance Ltd..

N. SUMMARY OF ENVISAGED ACTIONS

418. In summary, the corrective powers that I hereby exercise, by way of this Decision, are as follows:

(a) I order TTL, pursuant to Article 58(2)(d) GDPR, to bring its processing into compliance with the GDPR in the manner specified in this Decision. This should be done within three months of the date on which this Decision is notified to TTL;

(b) I issue a reprimand, pursuant to Article 58(2)(b) GDPR, to TTL regarding the infringements identified in this Decision; and

(c) I impose administrative fines totalling €345 million, as follows:

i. In respect of TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR **(Finding 1)**, a fine of €100 million.

ii. In respect of TTL's infringement of Articles 5(1)(f) and 25(1) **(Finding 3)**, a fine of €65 million.

iii. In respect of TTL's infringements of Articles 12(1) and 13(1)(e) **(Finding 5)**, a fine of €180 million.

419. In having selected, from within the fining ranges that are set out in Section M of this Decision, the specific amounts of the administrative fines to be imposed in respect of the infringements identified at a. to c., above, I have taken account of the following:

(a) My assessment of the individual circumstances of this particular Inquiry, as summarised earlier in this Decision;

(b) The purpose of the administrative fines, which, as noted earlier in this Decision, is to enforce compliance with the GDPR by sanctioning the infringements that were found to have occurred (effectiveness);

(c) The requirement for a genuinely deterrent effect, in terms of discouraging both TTL and others from committing the same infringements in the future (dissuasiveness);

(d) The requirement for any fine to be proportionate and to not exceed what is necessary to achieve the stated objective (as recorded at b., above). 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;

(e) The views expressed by the supervisory authorities of the Netherlands ("**NL SA**") and France ("**FR SA**"), 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. It is important to note, in this regard, that, contrary to TTL's position in the Final Submissions, 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 that might be expressed by a CSA, further to the circulation of 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. I note that NL SA's comment outlines its view that "*the lower end of the proposed range … would not be sufficiently dissuasive in this case. NL SA points to the unprecedented annual turnover figures of the ByteDance company … and finds that the low end of the range seem [sic] too insignificant in terms of percentage of the global turnover. Moreover, when regarding the field of data protection law, this case is likely to be among the largest enforcement cases possible, in terms of how many (under age) data subjects are affected by it throughout Europe and beyond. According to paragraph 333 [of the Draft Decision], it affected approximately* [redacted] *hildren. Hence, within the framework of the decision proposed by IE SA, NL SA is of the view that the maximum amount of 380 million euros must be imposed.*" The comment continues: "*(u)nder the GDPR, children merit special protection, and the controller in this case failed to guarantee that protection. In view [sic] of the NL SA, that is a further reason to impose the highest possible fine in this case.*" The comment of the FR SA similarly states that "*(g)iven the seriousness of the alleged breaches and the fact that individuals concerned are underage children, the CNIL thinks that the final amount of the administrative fine should be closer to 380 million euros.*"

(f) I have also taken account of the views expressed by TTL in the various submissions furnished on fining matters, including the Final Submissions. Insofar as the Final Submissions repeat submissions that were previously made by TTL and which have already been taken into account elsewhere in this Decision (such as, for example, submissions that the turnover of the undertaking is not identified by Article 83(2) GDPR as being a relevant factor in the determination of the fine amount), I do not consider it necessary to repeat my position on such previously assessed matters here. In relation to the comment of the NL SA, TTL submitted that "*the DPC did not find that* [redacted] *[Child Users] were affected by the public-by-default processing in paragraph 333 of the Draft Decision, as suggested by [the NL SA]. It is clearly not the case that all of these users elected not to opt to make their accounts private or that their decision was influenced or affected in the manner suggested.*" I note, in this regard, that Finding 1 corresponds to the DPC's findings, as regards the public-by-default settings for Child Users during the Relevant Period. The issue at the heart of Finding 1 – the public-by-default settings – affected all Child Users equally at the point of registration and immediately thereafter. While it might well be the case that some Child Users might have subsequently opted to switch to a private account, this does not alter the fact that they were exposed to the risks discussed above upon registration as a result of the default setting. In other words, Child Users were required to take an active step in order to opt-out of the default setting. Accordingly, I am not persuaded by TTL's submission, as regards its application to Finding 1. I consider, however, that it has merit in relation to Finding 3. This is because, as already noted above, the setting underlying the infringement represented by Finding 3 required the Child User to opt-in to the Family Pairing setting before the identified risks could be said to affect Child Users. While I have already taken this factor into account when determining the fining range corresponding to Finding 3, I consider

that it is important to reflect on the matter further at this juncture in circumstances where this factor stands in marked contrast to the position, as regards the numbers of data subjects that can be said to be affected by the subject-matter of Findings 1 and 5. Accordingly, I have taken TTL's submission into account when determining the specific amount of administrative fines to be imposed for Finding 3 by selecting an amount from the lower end of the range. TTL has further submitted that the assertion, in the NL SA's comment, that the business model behind the platform is "*predominantly based on the processing of personal data of its users for advertising purposes*" is not a relevant factor in the calculation of an administrative fine and that "*(m)oreover, TikTok's processing of user data for the purpose of advertising, whether with respect to children or otherwise, was not within the scope of the Inquiry and, as such, was not the subject of consideration by the DPC.*" While I disagree that such matters are not relevant in the context of the Article 83(2) GDPR assessment, I agree with TTL's submission that these matters were not within the scope of the within Inquiry and, accordingly, were not subject to examination by the DPC. In the circumstances, I agree that it would not be appropriate for me to take them into account when determining the specific amount of the administrative fines to be imposed and, for the avoidance of doubt, I confirm that I have not taken account of such matters as part of any aspect of the fining assessment.

(g) In relation to the FR SA's comment, TTL has submitted that the FR SA has not identified any relevant factors which have not already been taken into account by the DPC in proposing the fining ranges in the Draft Decision. TTL's view, in this regard, is that *"(w)ere the DPC to factor those elements in twice, this would constitute an error of law and would result in an administrative fine which is disproportionate and excessive.*[368]" It is important to remember, in this regard, that my final determination of the specific fine to be imposed, from within any previously 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 range(s) 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. Where any new factors are identified, further to submissions or otherwise, these matters may, of course, be taken into account as part of this final summation. The FR SA's comment indicated that the FR SA considers the "*seriousness of the alleged breaches and the fact that [the] individuals concerned are underage children*". I have taken this comment into account when selecting the final fines from within the proposed fining ranges. In relation to the matters addressed in paragraph 6.23 of the Final Submissions, I disagree that: *"(w)ere the DPC to have regard to the comment of the [FR SA] in its determination of the fine amount … it would also be necessary to have regard to [the FR SA's view that Finding 3 was not intentional in character], which does not support the imposition of a fine at the upper end of the range proposed by the DPC.*" I consider that the FR SA's comment must be read as a whole; in having disagreed with the DPC's characterisation of Finding 3, it logically follows that the FR SA's subsequent view that the final fines must be selected from the upper end of the proposed ranges was premised on its own view that all three findings were more appropriately classified as being negligent in

[368] The Final Submissions at [6.21].

character. I further note that FR SA's view, as regards the requirement for the final fines to be selected from the upper ranges, was informed by the two factors of significance that it identified in its comment, namely the seriousness of the infringements and the status of the affected data subjects as underage children. In other words, its view does not appear to have been significantly influenced by the characterisation of the infringements.

(h) Addressing the determination of the final fines to be imposed more generally, TTL has submitted that the fines ought to be selected from the lower end of the proposed fining range. Much of the relevant part of TTL's Final Submissions repeat submissions previously made and taken into account. As already set out above, I do not propose to repeat my consideration of any matters that were advanced by way of previous submissions and which have already been taken into account within the assessments of the criteria outlined by Articles 83(1) or (2) GDPR. I note, however, TTL's submissions regarding the changes made to the Family Pairing feature during the Relevant Period. TTL has submitted, in this regard, that, *"(i)n November 2020, TikTok changed the Family Pairing functionality so that direct messaging could not be enabled for 16 and 17 year old users … if they had disabled it*[369]*."* I note that this change was only in effect for a limited portion of the Relevant Period and that it only applied to a limited range of Child Users (being those aged 16 and 17 years of age). While I do not consider that this change was of such significance that it might require me to adjust the fining range that was proposed in response to Finding 3, I agree that it is a relevant consideration that I ought to take into account when selecting the specific amount to be imposed from the fining range and I confirm that I have done so by selecting an amount from the lower-range.

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

<u>This Decision is addressed to:</u>

TikTok Technology Limited
10 Earlsfort Terrace
Dublin 2, Ireland

Dated the 1st day of September 2023

Decision-Maker for the Commission:

[sent electronically, without signature]

Helen Dixon
Commissioner for Data Protection

[369] The Final Submissions at [6.26.6].

APPENDIX 1 – THE ARTICLE 65 DECISION