In tile matter of t he General Data Protection Re gulation DPC Inquiy R eference: TN-21-9-2

In the matter of TikTok Techn ology Lt mited

D4cI sion Of the 0a la Protection Comm issio n made purse ant to Action 111of the Data Protection Act, Z0IB and Articl es 60 an d 65 of the General Oata Protection ReguTatio n

Further to an own•yoIitIon inquiry commenced pursuant to Section T ¥0 of the Oata Protection Act, ZOTB

DECISION

Decision-Maker for the Commission:



Helen OI xon Commissioner for Data PtoteC ion

Dated the T" day of Septem ber, 2023



Data Rrotectlon Commission 73 Fitzwilliam Square South OubTin 2, Ireland

###### 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.\*
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.

###### SUMMARY OF FACTUAL BACKGROUND

1. 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

1. 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.’ TTL's sole shareholder is TikTok Information Technologies UK Limited. TTL's ultimate parent is ByteDance Ltd.6
2. 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
3. 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.
4. 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
5. 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
6. The collection and use of TikTok users’ personal information is described in the TikTok Privacy Policy.1\*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
7. Per TikTok's Terms of Service, users of the platform must be at least 13 years of age.1’ 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].

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].

1° 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.

1’ 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.

1. COMMENCEMENT AND SCOPE OF INQUIRY
   1. **The Inquiry**
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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”).**

1. 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”).**
2. 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”).**
3. 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.
4. 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
5. 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”).**
6. 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:
   1. The Italian SA raised an objection on 10 October 2022; and
   2. The Berlin SA (representing the views of the SAs of Berlin and Baden-Württemberg) raised an objection on 11 October 2022.
7. In addition, the following comments were exchanged:
   1. The Hungarian SA exchanged a comment on 10 October 2022;
   2. The Danish SA exchanged a comment on 11 October 2022;
   3. The Dutch SA exchanged a comment on 11 October 2022;
   4. The French SA exchanged a comment on 11 October 2022; and
   5. The Berlin SA exchanged a comment on 11 October 2022.
8. 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”).**
9. 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.

1. 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.
   1. Temporal Scope of the Inquiry
2. 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”).**
   1. Material Scope of the Inquiry
3. 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.
4. 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.

1. 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’.
2. 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.
3. 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.
   1. Assessment of TTL's Compliance with the GDPR and Corrective Powers
4. 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:
5. Firstly, in relation to platform settings:

* *Whether, having regard to the default public settings applied to Child Users' accounts, [TTLj 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, [TTLj 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, [TTLj 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’sj platform settings allowed an unverified non-Child User to access and control a Child User's platform settings, [TTLj 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*

1. Secondly, in relation to age verification:

* *Whether, having regard to[TTL'sj requirement that users of TikTok should be aged 13 and above, [TTLj 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'sj requirement that users of TikTok should be aged 13 and above, [TTLj 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'sj requirement that users of TikTok should be aged 13 and above, [TTLj 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.*

1. Thirdly, in relation to transparency:

* *Whether Child Users are appropriately made aware as a user of[...j 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[...j 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 1*

1. 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.

2° Statement of Issues at 11.

21 Statement of Issues at 13.

1. PRELIMINARY LEGAL AND PROCEDURAL ISSUES
   1. Competence of the DPC as Lead Supervisory Authority
2. 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.
3. Cross-border processing is defined in Article 4(23) GDPR as meaning either:
   1. *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*
   2. *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.*
4. 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.*

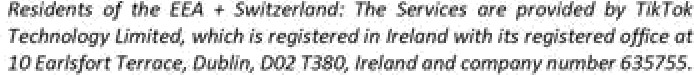
1. The TikTok Community Guidelines (December 2020) similarly provide that:

*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.*

1. 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.
2. 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.
3. 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”).*

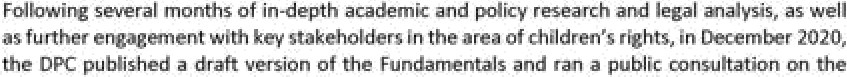
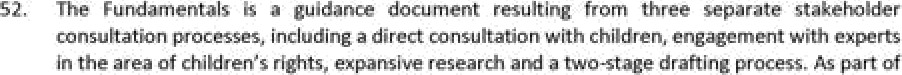
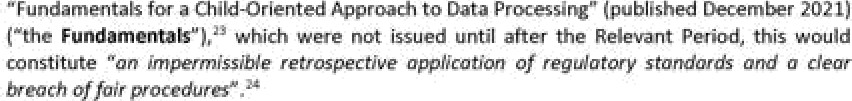


**

m. My cemfdemd dl ct the abcde aad the nsiure of d+e preen&q ct be, I or stifled tnzi



Js the s af @s mgNry. Tam krther that M has Ba man ecob¥slt t ln Leland fa the put of the GB is web, I em saflsfled that W rpu emerrts ef Argde ss G0Pfi has beonmet Tn elite the rocecsi at iacu arch that & DACIa nt to



##### \*O

1. 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.
2. 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.
3. 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.
4. 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.
5. **ASSESSMENT OF CERTAIN MATTERS CONCERNING ARTICLES** 5, 24 AND 25 GDPR
   1. Nature, Scope, Context and Purpose of the Processing
6. 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*

1. 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*

1. 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 The

approximate total average number of monthly EU TikTok users under the age of 18 was gyzs

1. 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 wa \*6 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 \*7
2. TTL does not hold statistics on users' account status beyond 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
3. 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\*’
4. 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.
5. 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 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*

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

2\*TTL initially indicated this number was 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.

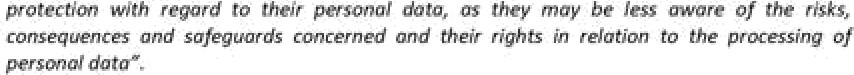
2‘ Response to the Notice of Commencement at [9.2.3].

\*7 Response to the Notice of Commencement at [9.2.4].

^ Response to the Notice of Commencement at [9.2.5].

\*’ Response to the Notice of Commencement at [9.2.6].

### . this Inquiry eeietoi to bo4i metered fillet mm who src ct tenet R pen clit rodp

than l8 yes end, ac wa4 zs cltfidmn under 13. mv GnP6 mcepiti+i chJi&un as o mlmiabk cateaorf ct eeoPie wid in pwttmlar ftecltoi R 00Pff notm that Aildren ’mwit

lmplanent a @wte ant uting M +s very dear that laugh mayN uaers







##### uzar wlahas ie opt Mr a phvae aoeocnt, users muct poly opt te do or mey 't@' his

dedWn and tied rrt is -ede WN It,’^ WI hay not opted to What the

### This end ft stfll pre te be a dei&ram cbehe en th pan ct Wt, intao&d te





w e•fi, It is not Uw h'ow cert Ultimate w specific reesom @ be pr+dermined by InvertNg auth a chotte, or dafauTtlng the acoo«nt to @vate.

1. 

##### come.“” Antler cs it oould be safd thet prIwte-by'-deFeuft would ally #Ifect thls, users

of a eel\* prgfif is public end nabo, thereby facilitate connects 8r•+ she sherlna

1. Cient bared publldy w 7@ok T¥ not I/mIted to uiers. Such c<mtwt /y also mede avails onthe 'rrab browser persian of a prafile pagz to an fndzt J+date global audénca of persons whole not bredusers Certaln cost on the web browser verslon cgn be on
2. In6 Response to W PID, Tlt dbputed the there wey puMli feuft process@ at II. ^ this was la nrst tfme tf+ft su6missJon waa mado, and coMrasted to the pious tubmlsslons made fo\lewIng the Stazemenz ot Sues, fa exeop¥ these excerpted above.^ Trdeed, thb

¥ubm\ssJon Is also /nconaWnt with othar statements that WI has made in thls negard.’^ Inarry

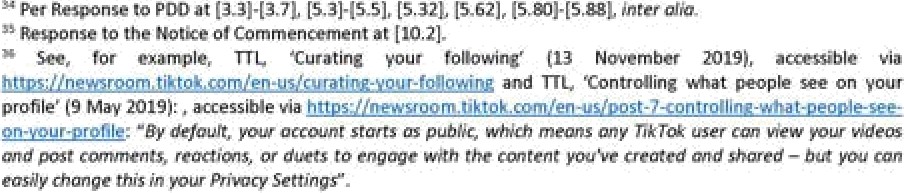
everrt, Tn the premises, it is not accepted that, as a matter of fact, an count 1s not public-tty-Weuft As at out et•ove, usm must pszltJ¥efy opt for y pr4wre acaount —the /y a cho •e that they must maLe in or-dw to av»ii of it or rf «y may ump+y nose to ’up’ tins decaion, in whfch

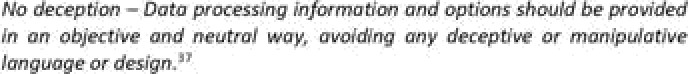
tfiefr gocount Is pu@Ic-by-dWñ.

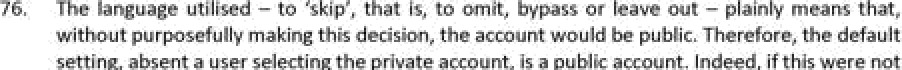
## 7S.

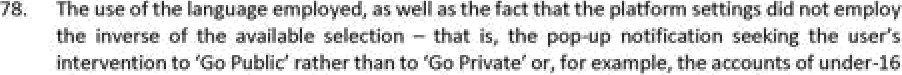






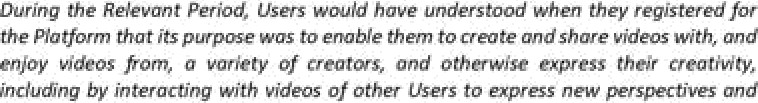
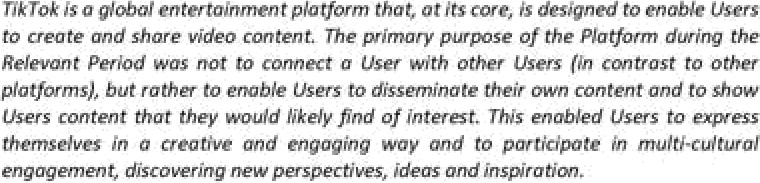






Pespome to tfie PDD Tntfd\* regardk klL w wit as ed othe respo«w gr+d mugs. Tgm of a ntonthzt Is ubflc •defsuIt for t asa reason I have ¥n bsl











*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. i...}4*

1. 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.
   1. Risks of varying likelihood and severity resulting from the processing
2. 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.
3. 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].

4° Submissions dated 14 April 2022 at [27].

1. 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.”*

1. 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*

1. 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.4* (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].

1. 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.
2. 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: This is applied

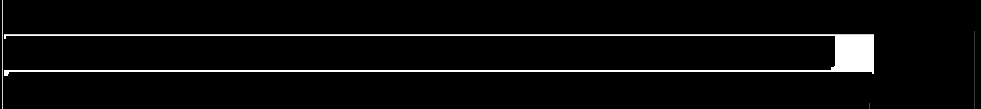
for both the Inherent Risk and the Residual Risk.

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

(a)

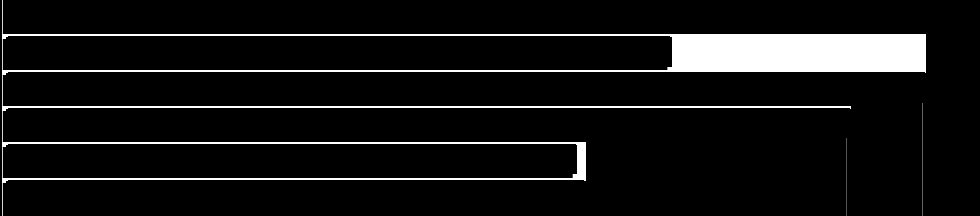
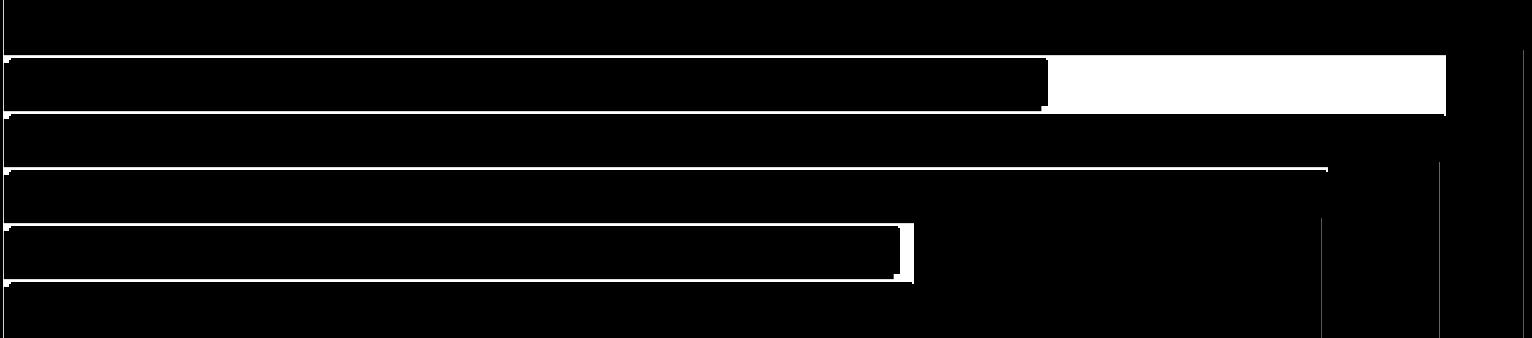
(b)

(c)



(d)

(e)



(f)

(8)

(h)

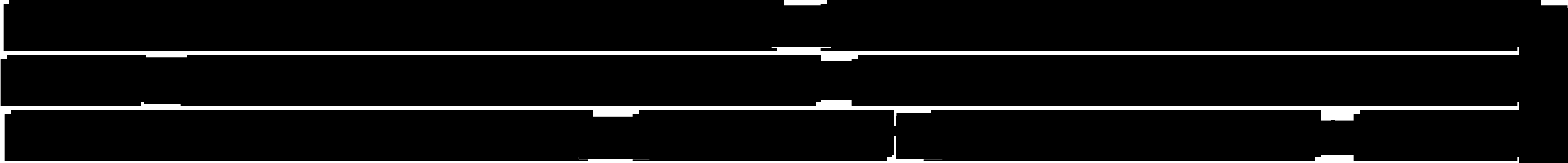
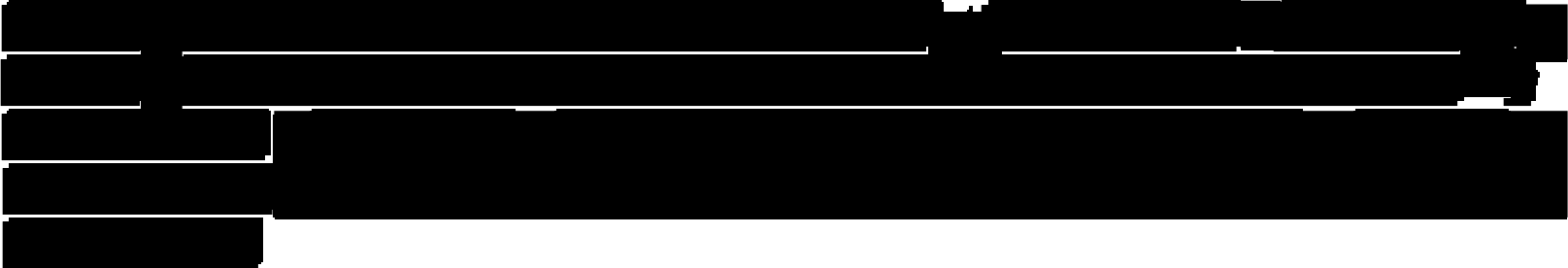
(i)

t:)

(k)

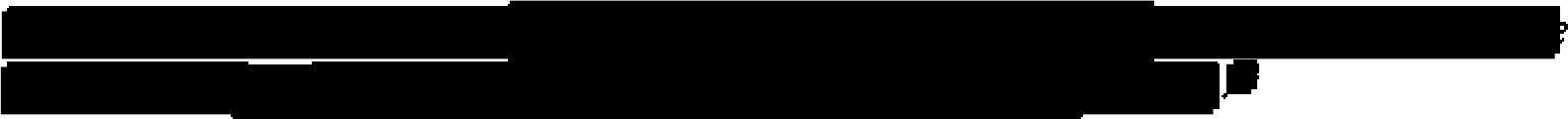
(i)

1. TTL identifies the In relation to its

mitigation measures including, as appropriate, the platform settings, TTL determines that the



°3 The DPIA at Part B, Schedule 2.



1. 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, ifnot addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss ofcontrol over their personal data or limitation of their rights, discrimination, identity thefi 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).4'

1. 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.
2. 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.
3. 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.
4. 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

\*° The DPIA at 15.

°’ 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.

1. 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.
2. 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 [beingj 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’sj 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*

1. 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.
2. 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.

1. 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, anv 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.
2. 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.
3. Accordingly, on the basis of the issues for determination, and indeed

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,

1. 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 DPIAs Iam 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.

1. 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.
2. 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
   1. Application of Articles 5, 24 and 25 GDPR
3. 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.
4. 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.
5. 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.
6. 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.*

1. 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 andfreedoms of natural persons.*

1. 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.*
2. 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*

e//ective.48d

1. 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.*

1. The obligation to implement measures and safeguards described in Article 25(1) GDPR is referred to as Data Protection by Design.
2. 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

1. 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.*

1. 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].

1. 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.
2. 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.’*

1. 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 andfreedoms 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*

’° 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.’1*

1. 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.’*

1. 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*

’1 Response to the Notice of Commencement at [13.2]—[13.5]. ’2 Submissions dated 14 April 2022 at [62]-[64].

*approach to data protection. The EDPB Article 25 Guidelines further state “[wjhen 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.”* [...]’3

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.’4*

*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.”*

1. 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 “[bjeing 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*

’3 Response to the Notice of Commencement at [13.6].

’4 Response to the Notice of Commencement at [13.10]-[13.11]. ”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./6*

1. All submissions made in this respect have been fully taken into consideration.
   1. **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*

1. 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.
2. 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.
3. 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.
4. 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.’7 It further stated that the user could change their preferences in the app settings at any time.’8
5. 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.’9

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

’7 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’.”*

’8 Response to the Notice of Commencement at [10.2]-[10.3] and Image 1 and 2. ’9 Response to the Notice of Commencement at [10.4]-[10.5] and Image 3.

1. 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.6\*
2. 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
3. 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 6!

1. 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

1. 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

6° 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].

6’ 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].

1. Private and public account user privacy preferences applied prospectively and could be changed by the user.70
2. 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.7\*
3. Users could block other users. This blocked all engagement from the blocked user, whether by comments, direct messages, follows or likes.73
4. 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
5. 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.7’
6. 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
7. 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

7° 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.

7’ 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].

1. 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*

1. *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*

1. *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*

1. *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*

1. *From January 2021, for younger Users aged 16 or 17, the download feature was turned “off”by default.*

*Suggest Your Account to Others*

1. *From January 2021, this setting is turned off for under 16 Users by default.’9*
2. 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.
3. 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.
4. 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].

8° 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.

1. 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.
2. 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:
3. the purpose of the platform and related context of the processing which would have informed Child Users' expectations;
4. 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;
5. the suite of privacy controls provided to all users, including Child Users;
6. the presentation of a user's video-level settings to the user before they posted a video (each time they posted a video);
7. the backend protections on the platform; and
8. the transparency information provided to Child Users.
9. 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.
10. 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:
11. the purpose of the platform and related context of the processing which would have informed Child Users' expectations;
12. 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;
13. the suite of privacy controls provided to all users, including Child Users;
14. the presentation of a user's video-level settings to the user before they posted a video (each time they posted a video);
15. the backend protections on the platform; and
16. the transparency information provided to Child Users.
17. 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.
18. 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.
19. 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.
20. 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:*

1. *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;*
2. *the required engagement with User controls before posting;*
3. *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;*
4. *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;*
5. *key aspects of how the Duet and Stitch features worked; and*
6. *the transparency information provided to younger Users.8*
7. 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
8. 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 i...} 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*

1. 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. i...}*

*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.8’*

1. 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 media86.
2. 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:
3. *Would a younger User understand the content of the Account Information Pop-Up and the First Post Pop-Up?*

8’ Response to the PDD at [5.131]-[5.141].

86 The Marwick Report at [1] and Appendix A

1. *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? 8’*
2. I have considered both the cover letter of 7 September 2022 and the Marwick Report in this regard.

*Analysis*

1. 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.
2. 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.
3. 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.
4. 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.

1. 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.

1. 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.
2. 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.
3. 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.
4. TTL notes there were approximately an average of egistered 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.
5. 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.
6. 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.

1. 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.
2. 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.
3. 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.
4. 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].

organTsaBonaT measures to ensore that, by defau/ only persortaT data wfidch were necessary

for TTt"s purple of procesflng were proceed.

Tn partfzuTar, dfis prozessirrg was performed to a glo6aT exteot md in érmmstances here TTS dld not Tmpfemwt meesum to enwre thac byIII,the zoclel medla conm of Child Users was nat made i6& (but tbe uWs irrrcwarréon} to an indefinite amber of natural persons. Tam therefore of o+e v4ew tbat the W•e processing by TTI was contrary to the prlntlpla of dna potectJon by'deafgnand default undor betide 25{1) and 25(2] GOPR, and c trary tp the data mñimisation pñnople order rUde 5(¥Xcl G-QPR.

 Frn- the purposes of assessirg Tra's comphace wnh Erlich 24 GDPR in relation to the pbIic• by-default Eng, \ Faye ansTdered the ngture. scope, conNxt end wrpose of the procesflng wfi •h rasolts from tfids tetflng, Hong considarad thesa Mr factors, I conduded tbat sha r• ocexsinB & tfie personal data af Mild Users results in a severe po@bk ms to the r gfirrs nd





t74. i do not a•cegt TTc's submlsslon 6et my assessment haa not properly tin Into account tea

/<e»anh ana -ea we and arken8 pnae<eom in aa ma‹zatea the ria‹ o‹

are some fnhere+it to ChiM Users on II+s intmet more gmeraI\, rum he T Failed to apprecJgte thgt unr Mred IkTN website use id at Seve the @l/ to comment on

bY non+egI\*tered arsons. It Is imply not wWngble to state that the #atform settNgs tfiet were tmplarnanmd ners T6erem w aIiOdId Uwrt gawraTly on the lr›tsmec

Further, TTI has speok fly refmed to IN+e 20¥B report by If+a just:raman esafety mBsWr, Wkh States thet 43% of children In tfie study Tnoeased ther pñ settings afar the precedTrg z2 months. Leayfog ask thet the audy Ts •G0PR andconcerns a ron•EU counts'. R <anot be Nferred. as WI contends that children made lnlermed choices, in a vacuum, to adduct ter cycaetlngs. Tbs orhw options amakiedTnthe ques8on• "taps‹ted sorrteow to rrry eel parents” ”biked sorrier”, "r geted Eomments^' etc. - suggest that chhdren are acting te an ordNe harm intended on sodas medla, ratkr tfiw making e c-hanBe on foot of tramparency irrformatl pzauided by thz controller. The rzgort does re+I su rt wbet TTI a suggested gnd,\ndeed, the CNIL study referenced gbove^ shows that r•›t all thiMren w care of the existence of privacy salgs and that cfidtdren have a preferaw

for private nano bydetaun.

 TTL hgs ow0kied the risk-bgnd meezures It ties Implemented for the pure of ensurlng gnd demons ata-ig its «om¢ance nich tie GDPR Cth regard to this esalng zhave ‹x nsfdsred these. wnfie \ gocegt that TTIpride certain Informabon, tools and Weguard\* to users, child Amata safety and praverg bad actors from Interactmg wlch Chlld Usan, Tam of the we that



against r<›nmi»iered user” utilising the we6 ite. I am th+t”etare af the that TTL he rx›t

perky tgkezt Inc scoount the nucs pond to the ftgbts end freedoms of Child Users wf+en



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.

1. 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:
     1. Manage screen time;
     2. Add more stringent restrictions on available content;
     3. Disable access to the search feature;
     4. Enable or disable direct messages for users over 16.
2. From November 2020, further functionality was added, as follows:
3. Make the account private if public;
4. Choose if the other users could view ‘Liked Videos’;
5. Limit comments;
6. Chose if the account could be suggested to Child Users.
7. 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].

1. 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.
2. 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 User9\*and, most centrally, that a Child User could have their settings made less private without their input.
3. 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.

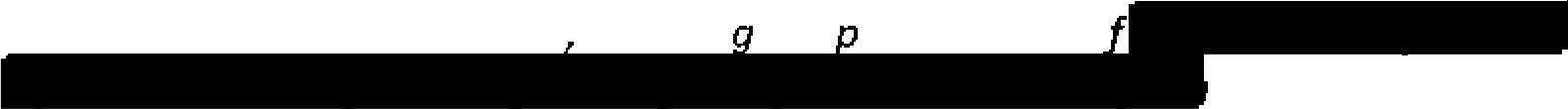
92 Response to the PDD at [5.136].

1. **ISSUE 2: ASSEMMENT AND CONSIDERATION OF MATTERS CONCERNING AGE**

#### VERIFICATION PURSUANT TO ARTICLES 24 AND 25 GDPR

**G.1AppIication of** Articles 24 and 25 GDPR

1. The relevant provisions in relation to Articles 24 and 25 GDPR are set out above.
2. 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 includin the otential use o*

*. 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.\**

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.*

1. Further:

’3 Response to the Notice of Commencement at [15.2]-[15.3]. ’° 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.”9’*

1. 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*

1. 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.

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

 Users of TikTok should be aged IN and above.'-" Y«r ir•g the period froa\ 2,0 J•Iy tO2O to 11 Occeml>cr Z020, Tip:Tot was rated in the Apple Aoo Stort os 't2+' and in the Guuglc Ptav 5Lor< as 'Parental Guidance Recommended'.

 Individuals wko wish to use TikTok must also confirm their date of birth via an age gas e. Inr/ividuals are asked to insert their dare or binh. No indication i5 provided for whr this is necessary nor does the select ion default to an age over J 5.”"

190 When individuals int 'r I u date Of birth bcl4w 13 y••\*» \* >8•, tht' registration pru os› t<aset. A pop-up notification states the individu al is not eligible for TikTok. lndividu aIs who seek to re-gotqr p g,$tg gf birtI\, yvhqthgr g bqvg qr @lqyr {}, try Why\yn thy Sga e • o\ i/ str a», a nd those who re-install the plaHcirm app *an* their device.^’

19I. Individuals under tr« ax< or za cho cntcreda date of birth abovc 15. II o 1s years gaincd

ac‹ess Lo the age-relevant plaEform seKings indicated above.

192. ouring fho oeriod from 29 July 2020 Eo 31 December 202g. TEL had a numbc'r *a\* measures tel remove users under the age of t3 who accessed Ehe platform. If TTL believed a user was under

13. they were rem ovco.\*

193 Frem d g les 2O2ü, is<rt a çt agn-gçgr$ ç iIg *repel a* se qngp/ } $ \ $iijg a yvpgfgr» gng yig the app."\*' This webform was called 'Requesr Privacy 1nform at ion', accessible via the ‘TikTok Help Centre’ and rI\e ‘TIkToL Saleta Centre“ on both the website and rhe app. Reported accounrs wero r c(crncd to muderators.

 T”â L also used o id+ntify if dn aCruurst wa4 held bv a us0J under 13 HHcrc such °"”' Where an account did. it alas referred to mede ation.

G95. If a mode+ator in another area considered a user wA5 under 13, they could refer rhe aero unr fnr

moderation ur ruuld *ackian* removaf of Lhi account thcrnnlvcs.'“”

 MudPr dti€H of an atco\int sutpettet\ to be op0rate•J by a user \inder 1”J i•\solved mudcr6tor5 having regard ¢o data such as theyMo-deral ors consider factors su‹h ask

” Rtwon5r \s \hr Notér oJ C<immrrir •msnt at I 14.II, Tik Tok, °TikTok 7rrms or 5rrvir'c' IJ uly ?‘O7O) anJ Td':Tod , °TikTo8 Privacy Potiw' jJulY 2020] and TTL's under-18s sum+riary of i\ s Privacy Policy.

fee oDnse to the tfDtI•ZE Of Commencement a I\*4. I ••\* Image 19. Response to the /6Dtice of Commencement a l14.4l ••d Image 20.

”” lie ance \a 1hr Naoce ar Cammrricem+rit JI I I4.5l.

! ^ 7rkTOk, 'Rdq \zE'£t PI?'s' X / Ir'i1ormalion' g€I°d'55ib4•D vsa !1!'J’'• '” ”a a a "ik I i’! .¿ ‹: iii •” \_'y.JI i-yr[r £ ”{i. i;. .i‹p .R ion If this rluring Wks Rclcvanl Period. a privac-y alice;›i••.i i ', i ik i'i•.‹ nri• mas made availabfe to uwrs Tar reporting gurpozes via the link n I th\*:,','”j'.;.x , li• to . nrr,”lry.aI,”r•› nr• ,'”pr• 4:', in addition *ta* the apg reporting, the Final Submissions at [&\*l.

' ' kes{›on5e to the Not Ee of Commenwment ar [L4.1ol and lubm lesions dated 14 Apnl 2oZZ at l1d 7l.

!" Suhm tfion< datrd I4 APrrI 2022 aI I137]. '\*' Response dated 21 February 2022 at 9.

1. TikTok does not require the provision of identity verification documentation in the registration process (for example, passport, national identity card, etc.).‘
2. 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 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 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

1. The Statement of Issues identified three matters for determination, in this regard.
2. 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.
3. 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:
   1. 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.
   2. If a Child User entered a date of birth corresponding to an age under 13 in the app,



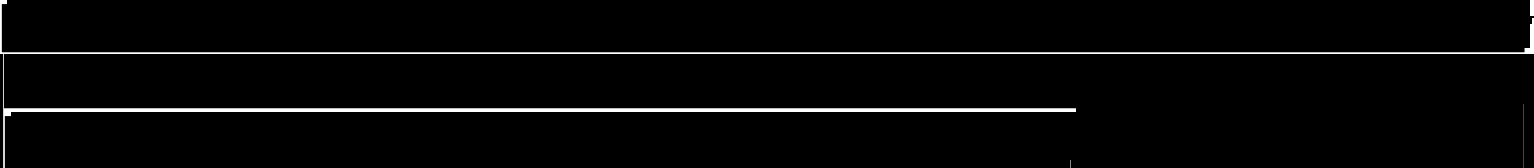
* 1. This was also implemented for users who signed in via a third-party account (e.g., Google, Facebook).
  2. TikTok was rated in the Apple App store as “12+” and in the Google Play store as “Parental Guidance Recommended”.
  3. When it was determined that an account had been created by someone who was under 13, the account was closed and deleted.

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

1 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.

* 1. 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.
  2. Where under 13 users were removed from the platform, a



1. 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.
2. 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.
3. 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.
4. 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.
5. 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

so that appropriate action may be undertaken.’OS

1. 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.‘06 As well as that:

1 Submissions dated 14 April 2022 at [140].

1 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.’*

*Analysis*

1. 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.
2. 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 children were detected as having gained access to the platform and were removed. This constitutes approximately f 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.
3. 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.
4. 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

1’7 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”.’0’ Aside from baldly stating this, this does not explain how or to what extent such risks were considered.

1. 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”.‘^’* 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.
2. 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.

1. 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.

1. 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,

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

1 Response to the PDD at [6.13].

1 Response to the PDD at [6.15].





Induduk iø e< Eu eaio føIi+a «gasasion on tł< belts of thsir ia+«tIęng as en kaMdusi

b•nłoøi L2 şøørź of egø 9nøx , besød nn m eąuørøh I smiÎ qpprnximøtsĘi wot'ø dotøct'cd M bøiøg tiitdot L3 cobio9uMt ID th•ør reg H xi zød removed

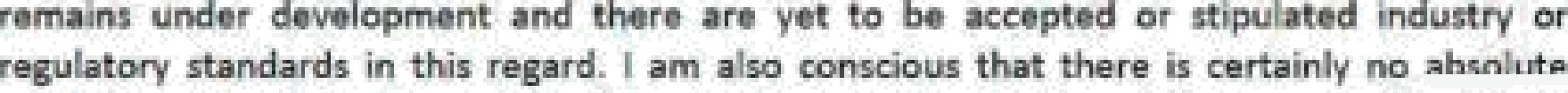
2J7. nets that WI dcd not employ chs usa oł ha•d Idaøtłflsrs Iø ordar te date dns the aga of ddldron aoæa6żng thø platform, however, I aoæpt TTL's auż›rr‹i6aizsn tźæt auch a raquizarrænt vrœńd bś dbproportlmate, glean thu ddklrsri, and partcu/arly yowøsr chddran, ers urăãtały to ż¥łzłd or /'¥øvó æóaas to such hœd identifiaTs end zips wæułd a<t to æîcltuJiztg cu• lorśóng out Dded Usan nho wouló o0›srw/zs ba abk æ utłlbs the platform, e well as thał”zuch e requiem would llkały &spropcxtónctały elf\set Chad Uzars from m›nerrty backgrounds. ^

 ki qzambing tt›s tccMical end ord meazuras identlflad by TTL, I am partiodzzfy

a asø” x+• zc ‹w zs sœa æ w. w «<aÿ «x, w

thct shotdd be • k order zo ensure aøs vartfI<atIz•n ar pnvsnt zł aa fпr sham

e p œm Ó r¥at intended to gsin æ æsa tø iŁ I am œnscńzustoo tżtat thø aras of agø varzfîcatzon



rnatkod of e vøucato«æ aat ń æ, Mb æ mø œ desæazrz•maør, tn sJatermrne a dæ

rnacsuras employed wars appropriate with regard to the ztøts of the ert, the œu of čnpkzmúriżaŁion æid tżæ natuïø, soópfs, arm+axe aru3 osøs of using asvatII as €Iae rîaka of. vawlng łikeiñæod and s•vsrky for rlğłtts end s of nabxsl persons poaad by”the



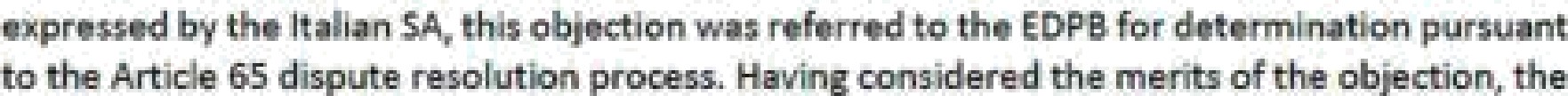
219. Acœrdkigły, on zhle basis, I poposad, in tins POD and ma Arcft D uon, to 8nd that the la tøîcøl æid organïxatîonøl maøsures in røsțz4słń of the egø vortf °tk›ri țæzxææas tJærnsałvzæ w›da+taáan by TTL dursng tea Rala aot Panod œmpład with the BDPg In lI$ I of the maaxires zmdaztzdian azzd tłæ extœrt to wha TTL sought to œmoæ”its pIatfó«m remained — œily

s3 cs/tob$a<iioøs zød ea Meg+ion ofaa Eœa h«tIzai æ& Arthe sf1şe\ aæae raæaon



# zæ. roik›«a the Eir»uieta« fW oon a æW csv a œ p«øw &eiæ aw to

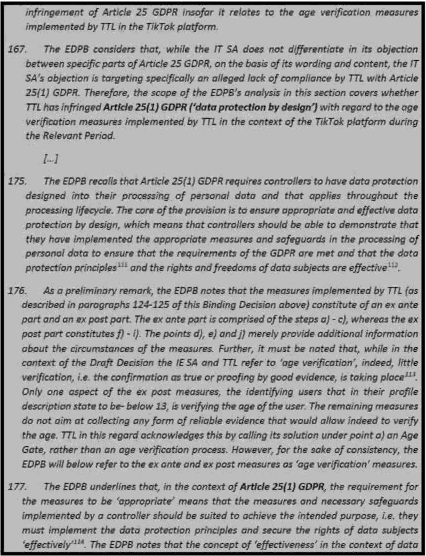
cxprsø \ ałr viaws In acccvdsncs with Aztlcls 60{8l GDPR, the Bśllan SA nizeó an ob}sctIcn œ



EOPBdwtwm wdæf‹ükwm:



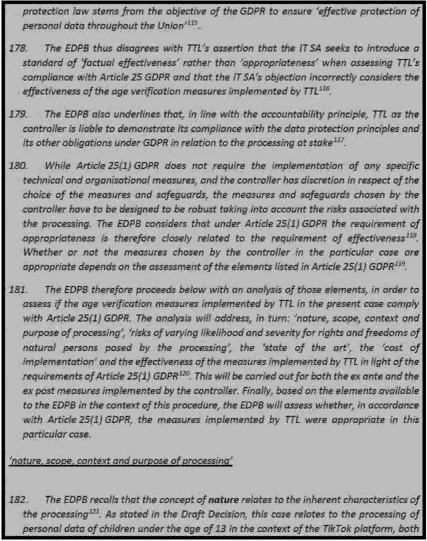
'•° fiespo•»e ‹a the fło î t of Coalat I‹x 7l and mis axle « i Z022 at [133I-lt39î.

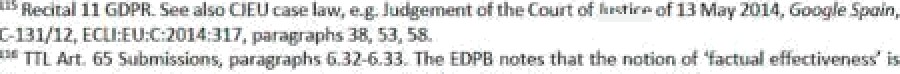


"’I++ dna a gig as tidied » u. s GoPft.

"’ EN Gwide ues ou Oata Pra4Wfon by 0eri@« and by 0eTaul4, VI.0, para r Z aud EOPB GufdeJM on Data Protection by 0efi$n aud by Defautt+ NZS. paragraph' Z.

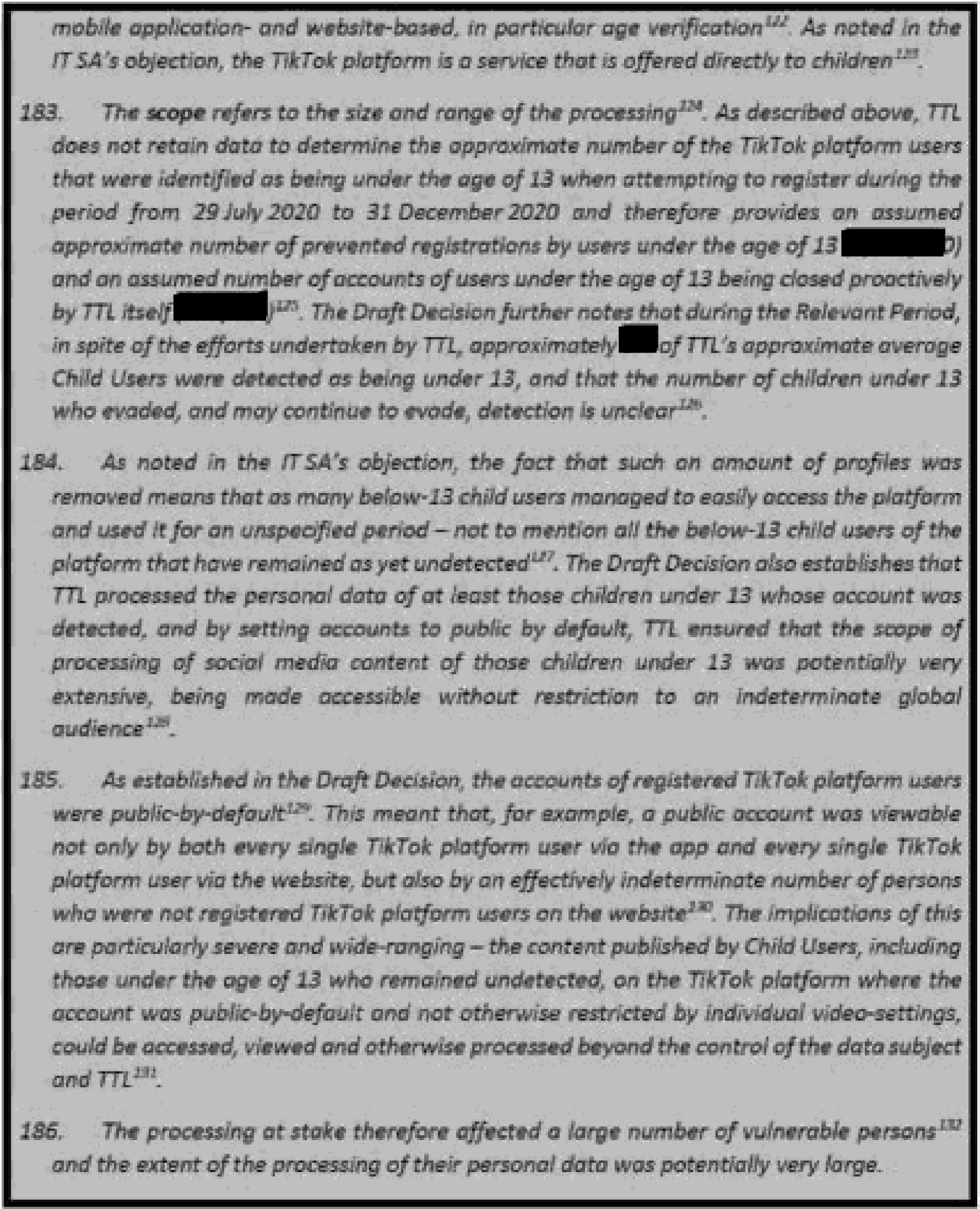
^^^ Sea defJnMo\*s In Oxford Fn$fâh'OIctT y





Jnrroduzad by TTL in Jun subndsuloro md is not reiesred To aT such Jn she TI @”a ob}ec\én. "’ srt. slzl ana a‹ c 4 soea, aeo se‹Aai 4 ¢zeir





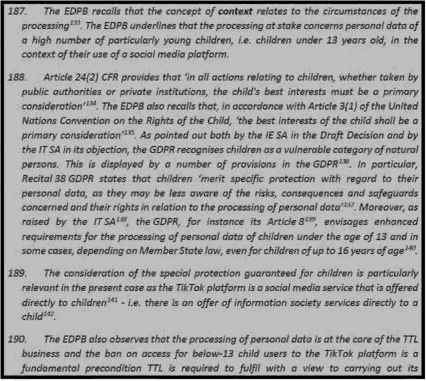


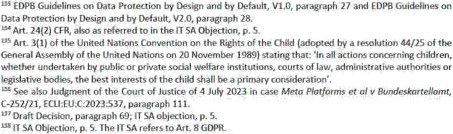
"’ EOPB Guidefines on oara Prolectiœs 0y 0esJgn and by De/aulr, 11.0, paragraph 27 and EDP8 Guideñnes oø Data Prolœtion 6y Oesign and by Default, V2ö, Paragraph ZB.

“’See Paph t7 7 af chb 8lru1Ing Di•cJsJcøt abœx•



fee this Binding 0e¢îsiorh paragraphs t2 7 a4 / t\*^\* above.





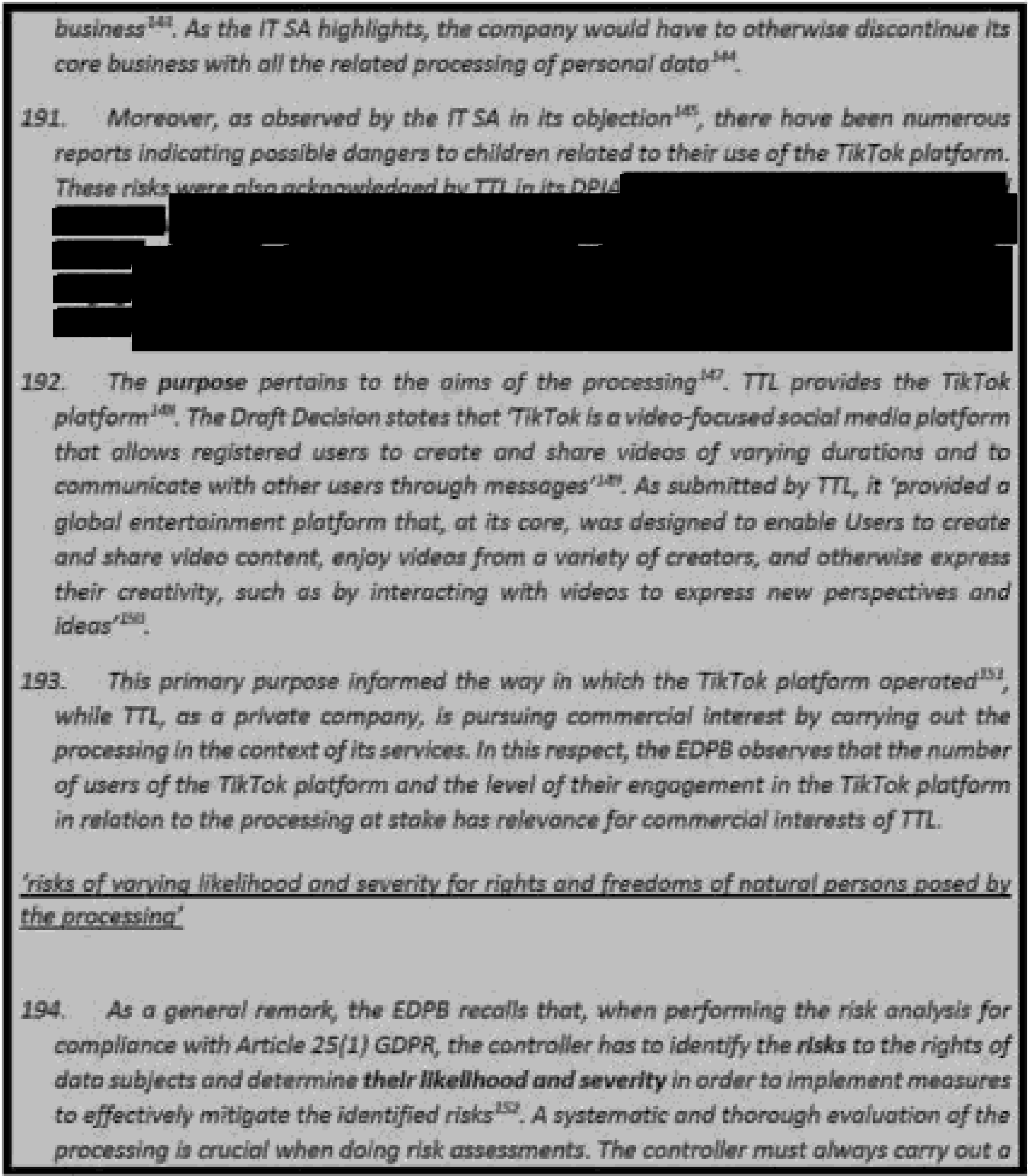
” x‹t. 8 l H GoPn. The E0ea aI« rub ii•at A r. cl jfl G0efi, referring ‹o the I fa proces»«•g censñtJng m the rracessity for dv of rhe fi+ezw imetW+ of ID's trdler or a Ufird pa+ty, iaiees fi panJcu@ the case +uhere tbe data ¥ub}e<z h a zhéd i\ W ‹annexe of W baWbtg caer t'é zo be zzrrJed aar by the coned. The E0P8 label recaks thai.é a data sub]erz. b a d\k¢, Ibid s éIaz+ a.iefeeni factor flu the

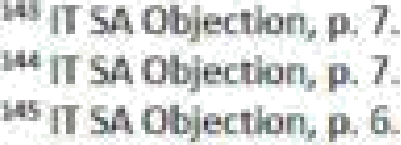
‹on‹roI!er ‹o the r•‹e sum w+›é•› «was w Art. 6NHbl uuPn, see roPB Gins Z/Zo 9 o« Art .6[ I){b} GB 13.

”A• t. 8{?} GDPR .

” IT SA Objndnn,g 6.

riacre'e ot»i, nr +‹niiu y a «aw neherb /›utroe nae‹1a m a





"TTLChildzPn's Oala arsd Age Apfsoorfa€e Oesign DPI Risir n. \ on p. Z1and Bidr n. 6 on p. 3B {on p. 32 and 39, TTL z/essr&rs the measures taten to nütigdIz• These risksl.

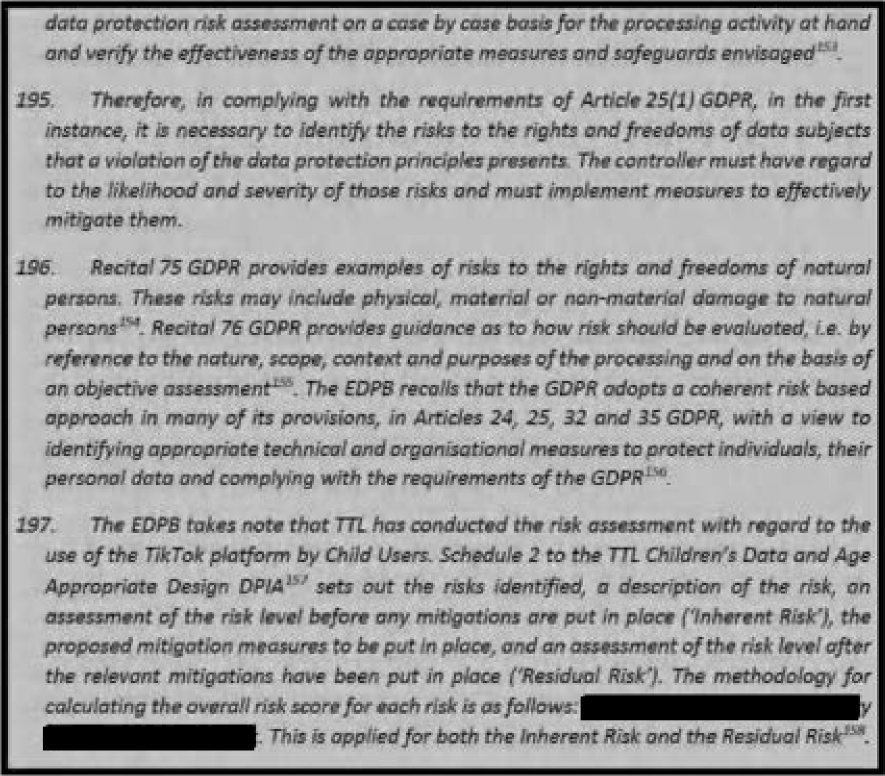
^’ E06'B GuI¢IeIlnm on Oazz Projectlo by 0eaJgu and by Defaulr, VG.0, pazagraph 27 and EDPB Guldetlnes az bata PratecrJon my Dedgn and by Di•faLdt. VDA.paragraph 28.

Kraft Destens, paragrap/ss 7 and 10.

”Oraft 0ecIs?cs, pafagraph 3, referring to TTLPDD 5ulxrfissJom, paragraphs 3.1-3.2.

TTLPDOSut›rrdssJonc, paiagraph 12.

E0P8 Gul¢Mlne on Dzra Prolectkxi ky Elestgfi and by Eie'kzulr. Vkß, pa agraPh 29 and £DPB Eulde Ines ön



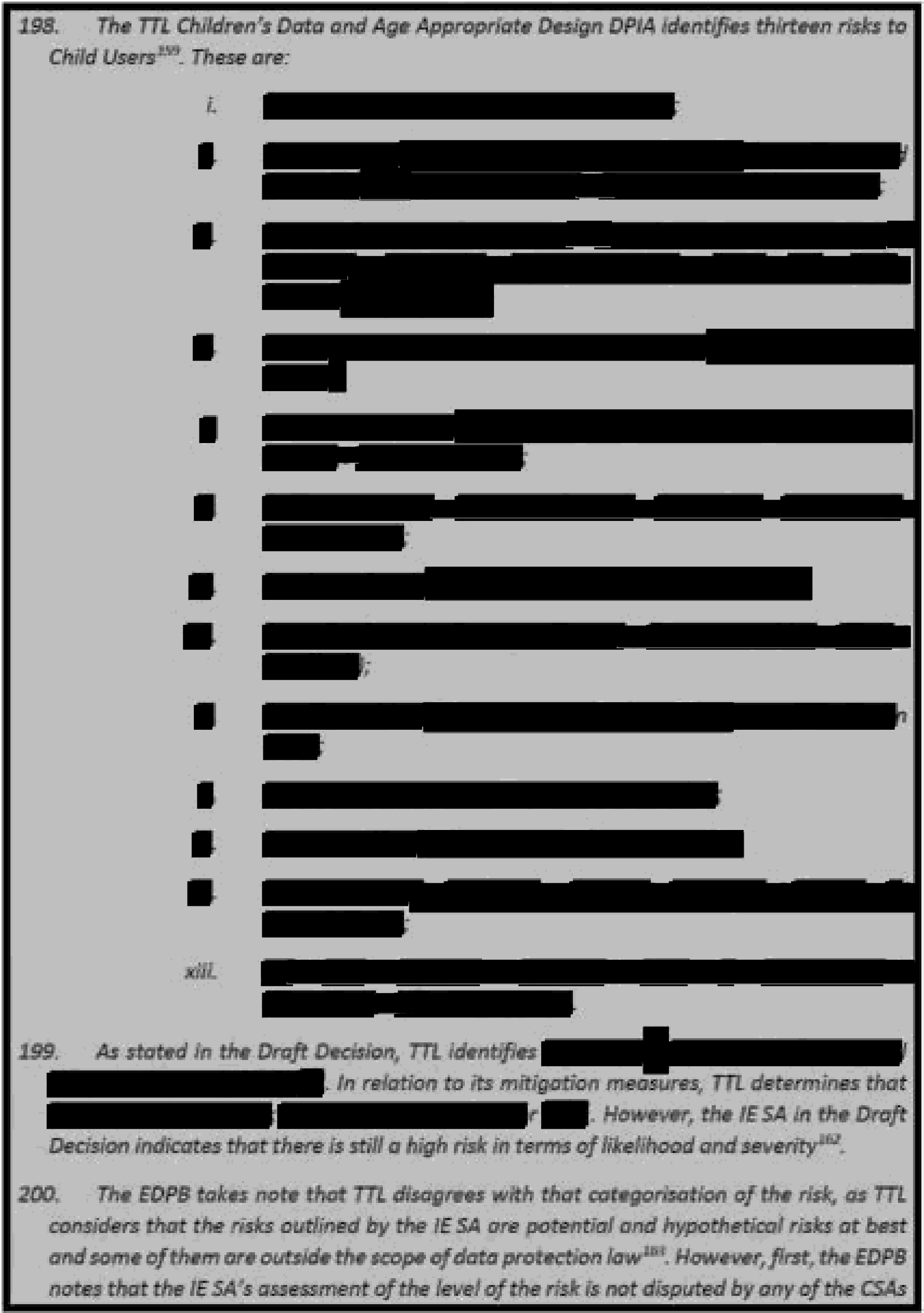


&eWtal76GDlNL

"EDPBfñsizMtnes on oau Pro\ection by' and b'y Oefaulr, VI.0, paragraph 2B and EOPB Cxside n”n on I¥ata Protestia•s by EI¥•sign a«\*d by default. VZg, paragraph 79, also stating \?›at\ ‘[i]he assetslo protect are a0¥¥ays t/u• same{Akeizu/ivJd via lfibprzrtect ci of zh”eir pPfszxsaJ data{, agañtst the same risks{la inâ?sñJua!s\* rlghcs}, tahmgInto acE l the sama cxxsdftlons [naiaxre, scope, context and p«poses of prozassllq)’.

” TTLChildren's Da£a Age **Appraptaie** @zugn £0KA, Schedule 2.

TTLChddren's Data arsd Age opñare Oeagri 091A. 1beduIe”A Part A.



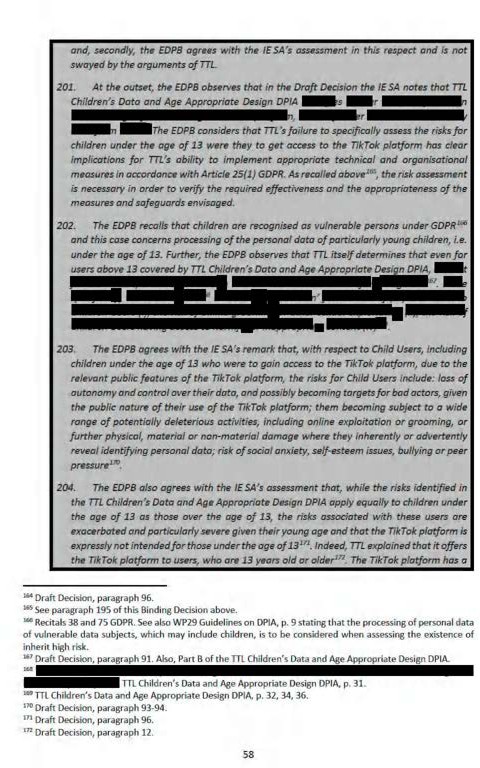
‘”’ TTLChi:Idreo's aaTa and Age Aop‹ooriaie Design DPIA at Pa•t B, S‹J'ieduIe 7; Draft Decision, z›aragraoh 90. "DraHDe<lsfon, p+ragra/d\* 9J.

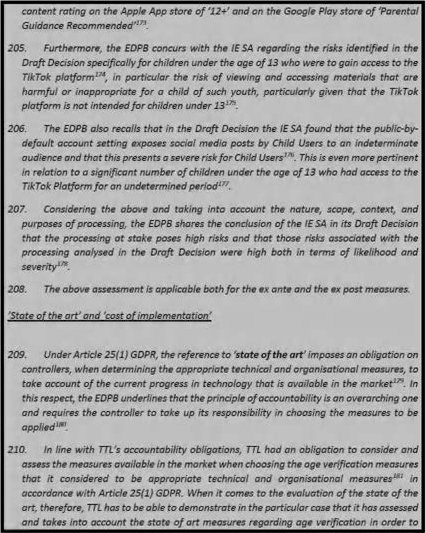
\*\* Drah 0ecisioi\, paiag‹aph 9l.

Drah DezIs¥zm. parag mph t43

‘^’ TTL PDD S\ibmi›ñoris, parajpaphs d 18-4.23.

57



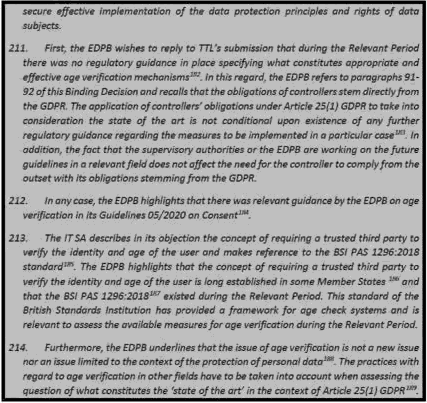


"• As bit from paaa@ache \83-184 aba +'e, a high r+umber oT cfii6r en under \Z years éld •r' . had as



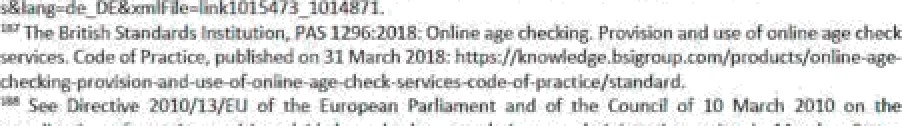
‘" £@B •' .:'ues ou Daca Protein Jzy and by Oefaub, VI g, Paph ¥9 and GB ' 'new w Oata Bzotectton diy Oedgn and by Defaul:.ISO. jsara$raph 14.







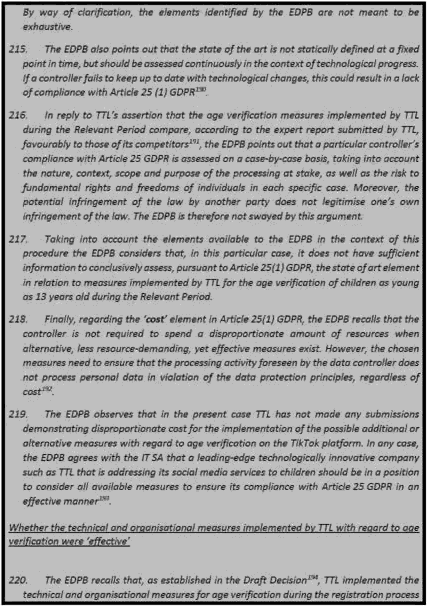
groce<tén by Das@n andby Gefzuh. PLO were abeq\ed on M 20tg1.e. prJor yo the Want Herod,



oire‹tie IEu› zele/taoa. i› p n in zes ‹hereof vx.its ›l us ›I-iaring run la, eng i+e

at es yh estabtlshkg arid operztin$ age Own. systems for ogre of video-sbaâkg gñatfcn nts

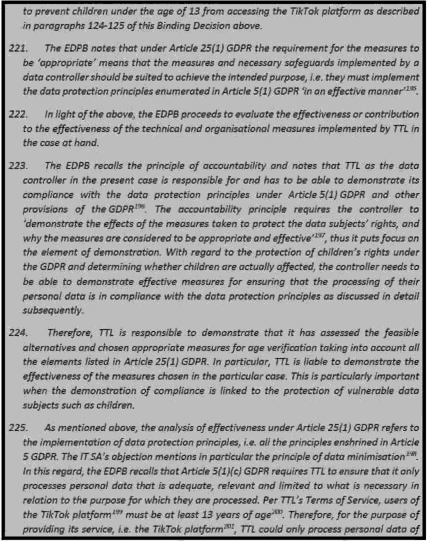
" £@B GfiideT\nes on Oara PiotWfon 0y and by 0efauK, W.0, paragraph' 72.

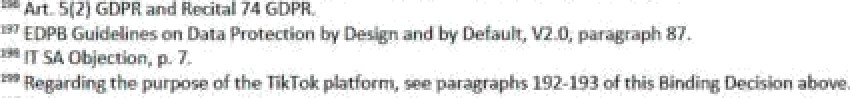




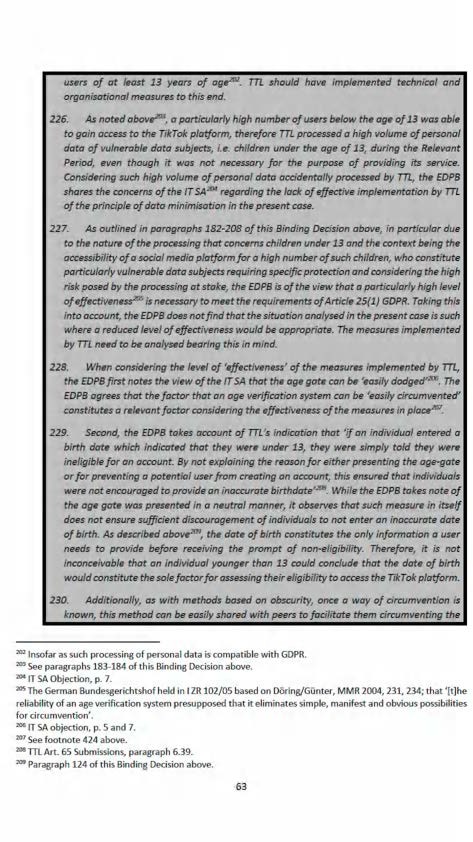
č@B Guk gines w Data 9totecúon òy and by 0ekauĘ Vit.0, pafagtaphs ź3-fiS.

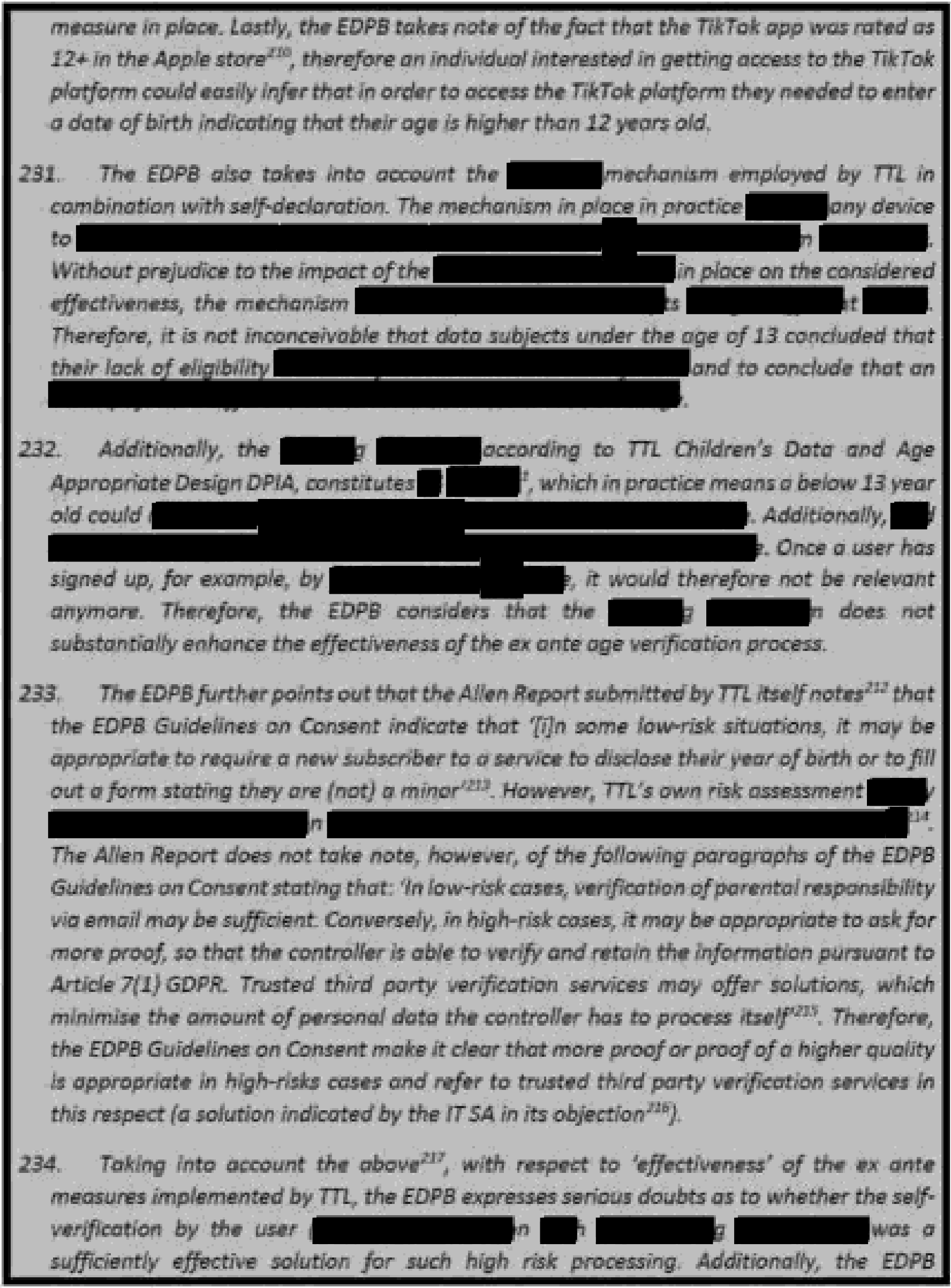
6ż





" bart W para@aph 5, referrir@ Tci TTt POD Wbmiséoug paragrap 'e 3. \-3-2 TTt PD0 Wóm 'e, pumaph 3.2. TukTn @&ded a i entertai platfnsm hurL at ire eve. rvo desagned fo enaW Uaers To creare lhe + den comeria, end vídeos from a vale+ry cf cseau and oóierwbe Wpress Im craatM£y,





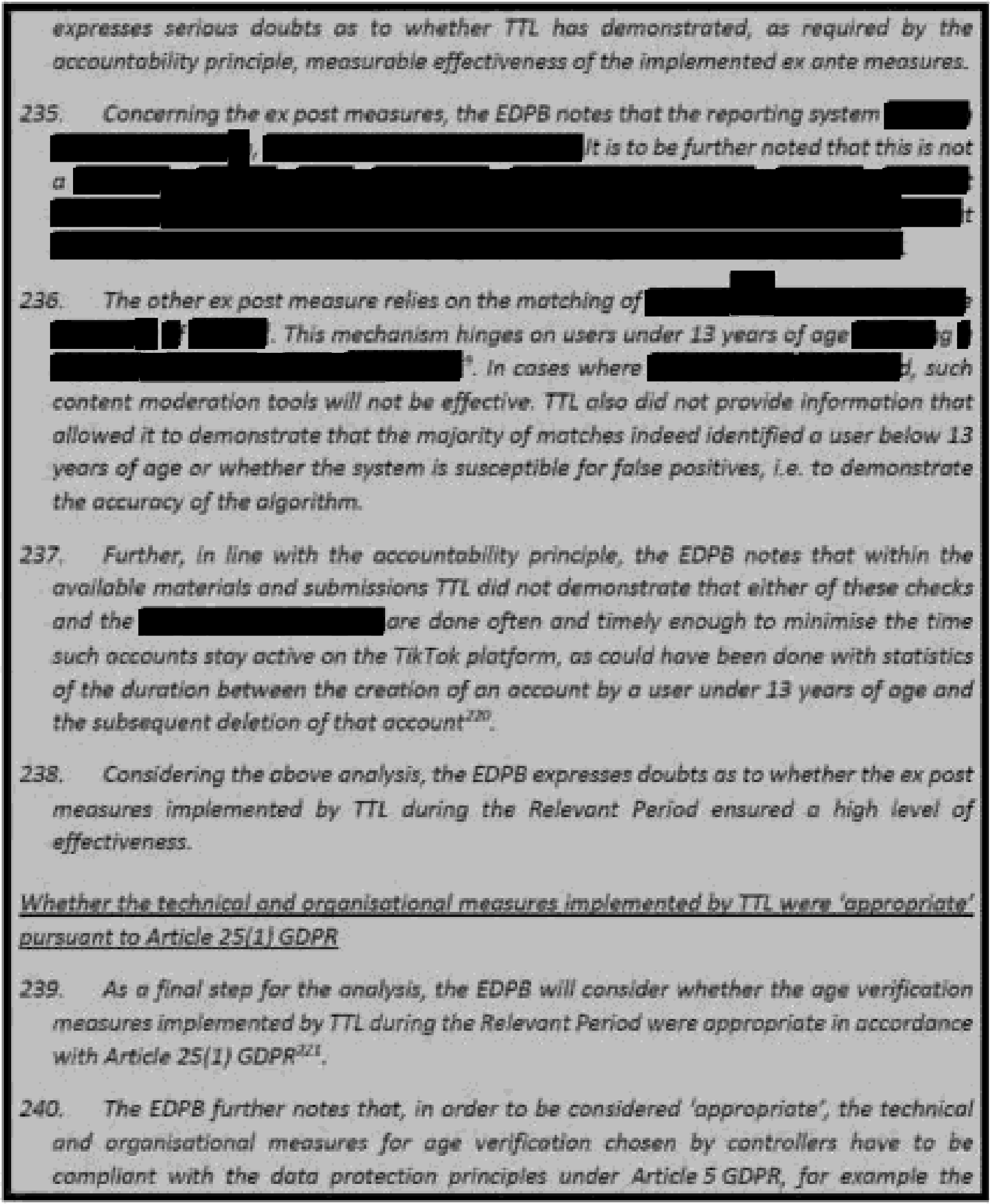
"\* TTLCh¥dren"s Oaca and Age Appropriate Deslgn 044A, p. Ii9. 3.a.e\I. The EDPB ncdes chai theDPIA mquesdzm a daied 8 Clamber 2020. therefore this dku»tkxi seems zo be apple ar Reset as of that momenE.

"’ A¥en Report. section 5.1.l.

£0f'B Guidelines on Consent, mph 133.

"’See paragraph \Z3 of this BirxJing Decision.

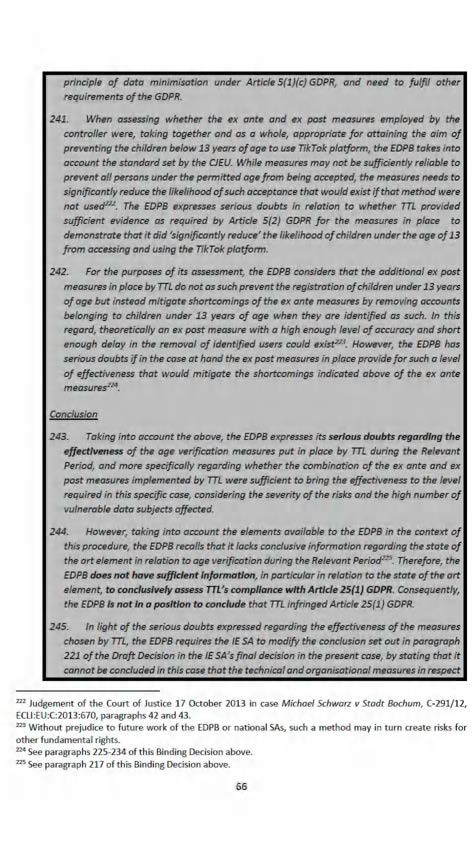
"’ ££tPB Gukti•lliies an Consan¢ paragraph 137. w

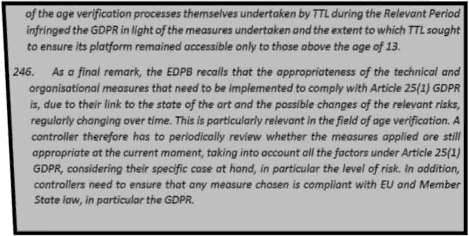


\*\*\* See paragraph 1JS al th& 8lndlng Eh«Jsicn.

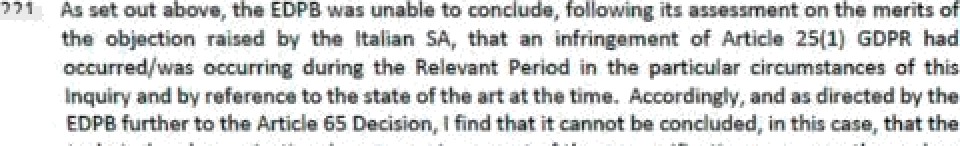
The E OPB rsores as we4I that some rime coukt be nPPded to pei4o‹m EhP in line wiih An. 72 GOPR, at\ae relevant whlh coukl be nai d«›e la an hsue unzfer Art. 22 GDPA, bu‹ chP resub of ‹hP ez poor use ol zamenr rnederadan measures to rzvnedy o sñorzc¢xrik+g, in. the regiszrarJon of a user wiih age below

“’ In this rega+d tle EDPB lakes no\+• of TTL"s view tlaat th+• ox•esures irnp •rneoted nPed \s k•ad to an aogroprJate k•¥óI of Pffecrńre«wss and rertainty al assessing the age, and not an aósólule Ie '‹nl of ‹z•r1ainiy{TTL Art. 6S Submissłoas, pa‹agraph 6.32}. I-h›tvever. as evłden‹ from the assescme¥+I n che sub-sectxm 14.Jal \hh Blru:łlng Dec , ihe E0P8 h assesslrig the nieasufe+ Im ed by TTŁ now agalnst an -\*hsnb t • 1evcl of cerraiłsry and ef1śctńreness. bu1 against ąn 'appeogsiabP’ leyeł as emńsaged in Ąrt”x e 75[1) Gg'PR.













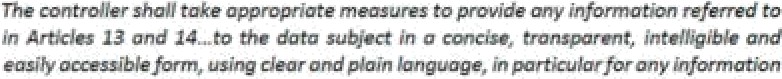
*H.* 6SUE 3 ASMSSMEMT AHD Cot¥St0ERAïtOM OF MAïTE4S C€IN€¥RKIF+G

3¥tArlsPa4DacY I•uItSu«t4T ïO nPFICLES 5 zz D IS 6O¥It



22a The GDBR restà e't pl alta must b+ ,/b ono' in o tro•aH›m•t

mgnnw In tWóhmt fio b¥a dóbo .’ SpeeWo GDPR pwzv%Mna gm èd in Azó@m







’ TTL TIkÏJ RNary 9u'l '/.

TTL TMTn Mm for \Jsers 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:*

* + 1. *the recipients or categories of recipients of the personal data, if any*

1. 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;*

* + 1. *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.*

1. 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.\*\*9
2. 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”. 3*

1. 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”. 31*

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

*Overview of Issues and Transparency Compliance*

1. 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.
2. This navigated to the confirmation of phone number, if used, and the selection of a password and username.
3. These documents were further available on the platform on the settings page.\*3\*
4. 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.
5. 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.\*33
6. TTL also had a ‘Youth Portal’, intended to provide account security information.\*34
7. 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

23° 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.\*3’

1. TTL also had a portal for parents.\*36
2. 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.\*37
3. I will now consider whether TTL has complied with two particular transparency obligations under the GDPR.
4. 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.
5. 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:
   1. Through its Privacy Policy, which was available during the registration process and in the settings and privacy tab;
   2. Through its “Summary for Users U18”;
   3. Through ‘just-in-time’ notifications;
   4. By presenting to Child Users their adjustable settings at the point immediately before they posted a video;
   5. 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;
   6. 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
   7. Through additional measures such as the ‘Help Centre’, ‘Safety Centre’, a Parent Portal and Youth Portal.
6. 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

23aResponse 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.

1. In this regard, TTL provided information to its Child Users regarding default account settings in the following ways:
   1. Through its Privacy Policy, which was available during the registration process and in the settings and privacy tab;
   2. Through its “Summary for Users U18”;
   3. Through ‘just-in-time’ notifications;
   4. By presenting to Child Users their adjustable settings at the point immediately before they posted a video;
   5. 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;
   6. 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
   7. Through additional measures such as the ‘Help Centre’, ‘Safety Centre’, a Parent Portal and Youth Portal.
2. 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 Plat(orm 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:*

1. *it was provided in a concise and transparent form;*
2. *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*
3. *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) 38*
4. 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:

*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?* \*39

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

*Both are written in clear language that 13—17-year-olds can understand;*

1. *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;*
2. *The pop-ups adhere to best practices when designing the language and placement of social media affordances for teenagers.*
3. In relation to the second question, the Marwick Report states that:
   1. *Young people are knowledgeable about the implications of posting “public”content online.*
   2. *This language appears in privacy curricula in use across the EU.*
   3. *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.*
4. In relation to young people's understanding of privacy,\*40 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. i...}*

[...] *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. 41*

1. In relation to digital competency and privacy education,\*4\*the Marwick Report states:

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

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.

24° 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. i...}*

*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.\*43

1. In relation to Child Users’ understanding of the ‘Public’, ‘Private’, ‘Anyone’, and ‘Everyone’,\*44 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. [...j*

*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”. 4’*

1. Finally, the Marwick Report states that Child Users respond to clear and simple language, and that the terms employed by TTL are so.\*46

*Analysis*

1. 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.
2. 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].

24’ 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.

1. 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. Ifi 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.*

1. 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.\*47 It states:

*Other TikTok users - Ifiyour 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].



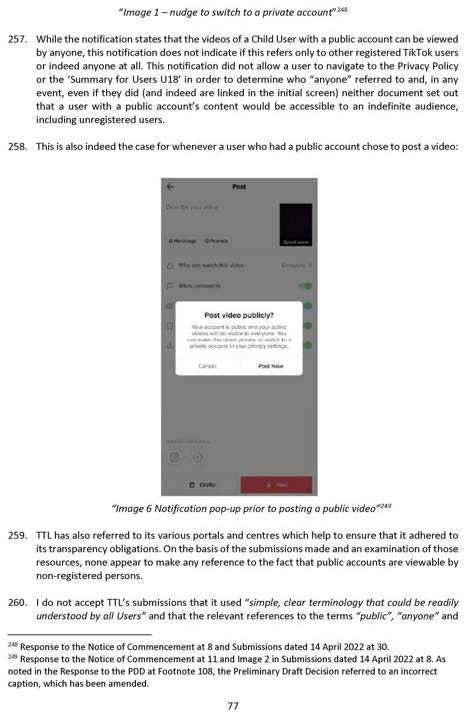
 while b9th d -end note that, where a+)ser opts for a 9•blic aocoum, the content posted on It Is accessible to any other our, nehher sat out at all thet, sfiould any user have a publlc. account, that account will be viewable the TikTok website by an indefinite number of persons otber then levered usen.

256. w£ also states thet what It terms gust in tfme' r•otifIcetfona were alt utilised so ensue thet It mat Its ttansparmcy org one. In tfiis parta•uIar context TTI has sit out the regTstrafion pnscM arid the variety o4 notify-ations rMating to publin and private account settfrjgs that it preserrtc TTI hx W out the process 'for th Istratk›o of users in had\* subm/wlons. Upon dri^rrrdoadIng the r«ogiIa application, users were presented wfth The various options for ggerdng an agcpnt using Qffferent greaen£ials and were pre•a• ed with Ilrrks to the Privacy













paragraph 7.20 ef the Roys to the PDO. TTL nefers a• Imege 9 winch see ”Age @fl be tosez canñmts zu//Aes. XouT# eo/rrogerzrzedñs oppr ze ners.”Tha adrBtionaT comext woukl suggest thet TTI was only refering to tegbtered uwrs, rather tben enyone rt gg.

 with regard to uan•id‹ aepert. na•iriB considered it in DII and tfie Ir•di•id gl aspects tnat Its concfuslora rest upon, wMIe Tdonot disagree a'gh enumber of Ita polna, I w not persuaded with regard to ñ.y clusipns. First, in relabon to your@ peop4e’s un ndfnB of prTuaz'y,

o efe i ilme thtt the nepoft refe›sto u th r•csrd east i woula azegree wnt. hiz not aenW



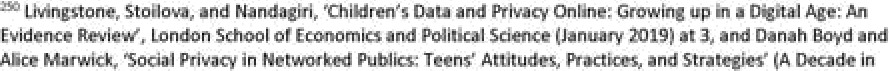
it is tear that, givzn the dines ge in digital Ifterazy across the Euro@ean Union. discussed below, between dffterem grwpGgs, gnd on tbe besls of ege, as web esthe belgne required to be faced between the value dtTldran plea on pr acy and fat thoy also desire two @l to engaae onkw,' tbe more necessary ft tz thet the @vecy 6pflcatlony e4 features are made deer and the Tn Tttelf undetl¥es tha ve central rele and ebll on oF trails re In tea GDBB. Sfmgfy bezartse zhfldren are privacy-a+u& e couM not Tn Jtsélf mean the ob1 lone under Articles 12 end 13 GDPR ale sullied, ad ough gwawes\* of the Imponem end fnctlon of p ”i•acy settings is of course, an important asge¢t of the ob]ectfves sought to be actfieued by Ardiles 12 gnd 13 GDP

” arwnd'throughout the Eur n Uni, agar I do not d rea that aching use tbs

European Unfon Is ñcreasi fncorgoratfrjg d@ftaT zompetenzy md prfvaz'y lrrto currieuTa.

£+owever, wRhN the meteflgT shed upon and relemced \n the Med Report ft Iz clear thgt aM authors arc cawei a note that the eae«t of sea literacy and add is uwverdy Wrlbuted vxy\ng wW, ewomlc end geographic stratg. Indeed, the Marwick fieport

racers to the “EU W Online {20 Mancfi 2020) pdm@ly Hsofar as to stata that 79a of





lnBmet firne: Lynn m on z e 0ynamJes of the Tnzernet aud 5oÖety, Oxfad, Engbn4, Z011) at 2ß

” Smahel, es a\ ’EU Es ßnf ue kruey flecuhs freo 14 Und (Erde 2 20s auai|abIe at



*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%).”*

1. 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. ’*

1. 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. ’3*

1. 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 i...} many users are not confident that they can configure their settings to obtain a desired level of privacy i...} Even when people do configure their settings correctly, information can still slip through the cracks. ’4*

1. 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

2’2 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.

2’3 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.

2’4 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.

1. 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.
2. 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”, \* 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.
3. 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.
4. 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.

1. 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’.
2. 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.
3. 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.

1. 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.
2. 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” ”* 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”),\*’6** 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.*

* 1. *The EDPB also notes that transparency is an expression of the principle offairness 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.*
  2. *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, “[tjransparency 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”.*

2” Article 29 Data Protection Working Party, ‘Guidelines on transparency under Regulation 2016/679’ WP 260 rev.01 (Revised 11 April 2018) at [1].

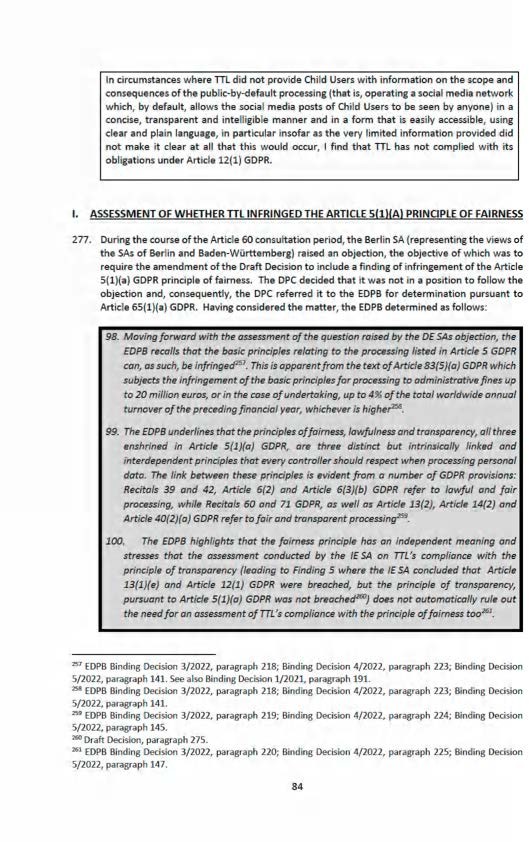
2’6 European Data Protection Board, ‘Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR’ (Adopted 28 July 2021).

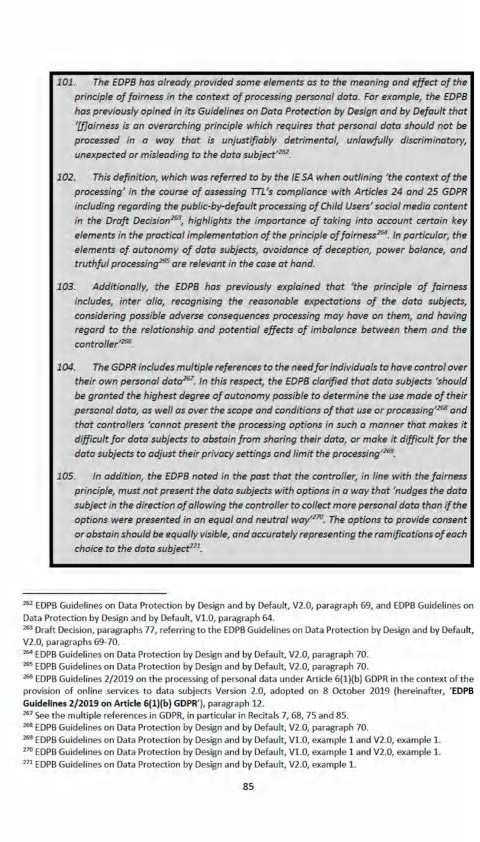
* 1. *This being said, it is important to differentiate between obligations stemming from the principle of transparency and the principle itself. The text of the GDPR makes this distinction, by enshrining transparency as one of the core principles under Article 5(1)(a) GDPR on the one hand, and assigning 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.*
  2. *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.*
  3. *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.”*

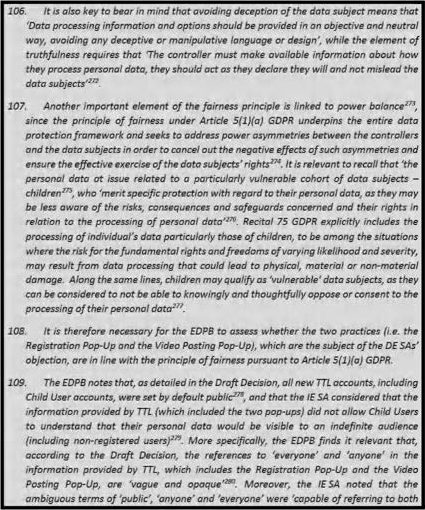
1. In the particular circumstances, I do not consider that TTL's informational deficits constitute an infringement of Article 5(1)(a). This is because, while the infringements of Articles 12(1) and 13(1)(e) GDPR are serious in nature, they are not of such a nature that they extend beyond the confines 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).

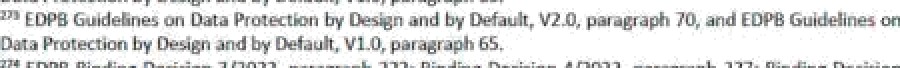
**Finding 5**

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.





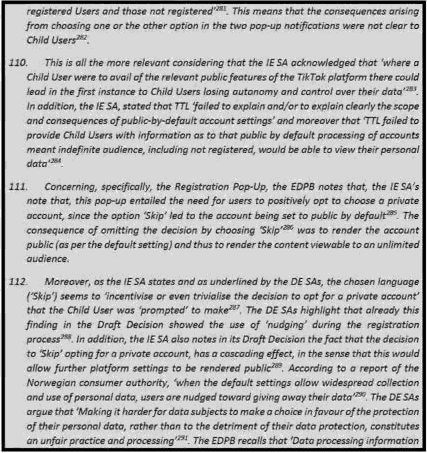






key.Ł, {heień-iahe• @ W Œ^tß“} endr+reed by W EOPB on 25 May 207$, g. @.



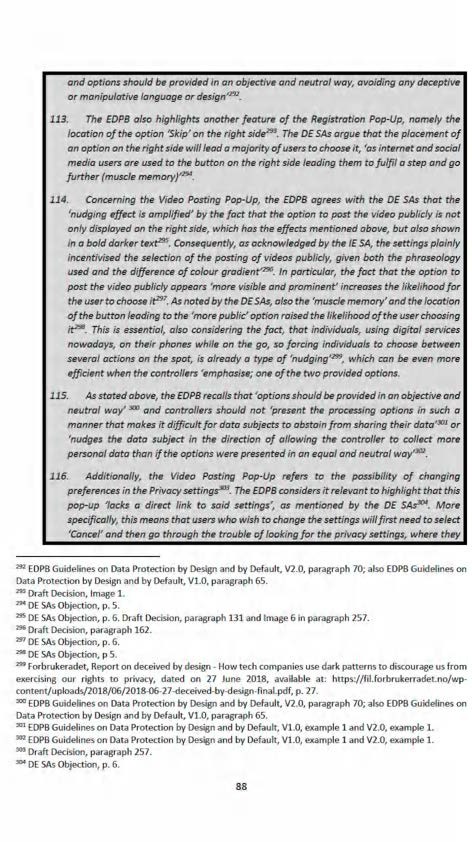


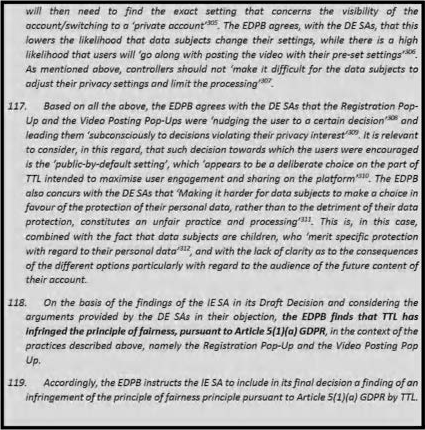
Tait GecJsIs, IN+dk+g seccmd part {'In cl cumsrar<es where ITL dld not pea+nde €Agd fleets wiki InformetIrs\ on the md cruaeque+ices of the pubic-by-defauh:gWeasJrig{tbaT @ data aFiat medTo

trampareu4, Intl Ie and easdy access¥ñe deal and plañi . in Star brsoksr a 4 'e ver iimkea c somatic aaea aa w maex ciear at u eat th\* occw i red that TTI bas mi

^’ 0raR Declsl<us] peagraph 16 +. DF jean. p. S.

"Forbr era.Repos on deceived by - He+w tech cafes use dark ferns 4o rgsreura e W morn emtci»in$ our r s a drivey, dated on 27 June 2018. avaBa gr ac! hrrps g8.forb+u ewadet.no/@-concmt/uploa dq/20t8/0 i/2&t8&-27-decetvñd-by-desk@\-final.pdf. p. IN





27B . Accoidrngly, arid a s directed by the £D PB hurther to the Article 65 Oec ision , \ fi nd that TTL flat

inft i’4^d the princiel¥ of feirno6s Comment to Art?te 5(l]Ie] G0fiA.









###### CORRECTIVE POWERS

1. 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.
2. 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.
3. 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.
4. 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.
5. 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...*

1. 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:
   1. An order pursuant to Article 58(2)(d) to TTL to bring its processing into compliance with the GDPR in the manner specified below;
   2. A reprimand pursuant to Article 58(2)(b) of the GDPR; and
   3. Three administrative fines in the range of €55 million to €100 million, €55 million to €100 million, and €110 million to €180 million, respectively.
2. 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.
3. 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.

###### ORDER TO BRING PROCESSING INTO COMPLIANCE

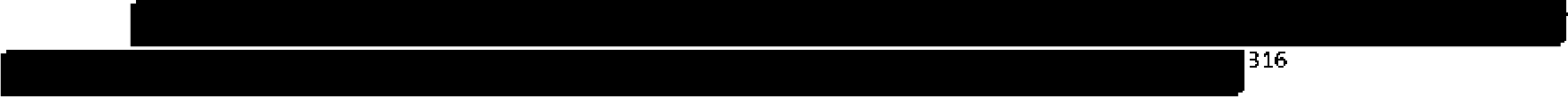
1. Article 58(2)(d) GDPR provides that a supervisory authority shall have the power:

*“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”*

1. 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.
2. 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:
   1. 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.
   2. 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.
   3. 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.
3. 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.
   1. Additional service modifications since the Relevant Period
4. 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.
5. 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].

1. 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 “offi’ by default. Finally, from January 2021, the ‘Suggest Your Account to Others’ setting is turned off for under-16 users by default.3’°
2. 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.\*"
3. Finally, with respect to age verification measures, TTL states that it is currently proposing to



build a

1. 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.^\*7
   1. Conclusion on the order to bring processing into compliance
2. 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.
3. 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.
4. 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].

’1\*Submissions dated 14 April 2022 at (128].

316 Submissions dated 14 April 2022 at [140].

’17 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.

1. 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 [DPCj”. \* 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*

1. 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.3\*0 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.
2. 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].

32° *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.

1. REPRIMAND
2. 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”*

1. 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.3\*1 For the reasons set out in detail in relation to each finding above, I do not accept this.
2. 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.
3. 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.
4. ADMINISTRATIVE FINE
5. 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”*

1. 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.
2. 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.”*

1. 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:
   1. *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;*
   2. *the intentional or negligent character of the infringement;*
   3. *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
   4. *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;*
   5. *any relevant previous infringements by the controller or processor;*
   6. *the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
   7. *the categories of personal data affected by the infringement;*
   8. *the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
   9. *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;*
   10. *adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*
   11. *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.*
2. 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.
3. 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.

* 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

1. 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.
2. 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 the

approximate total average number of monthly EU TikTok users under the age of 18 was

°2\*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 .\*\*^ 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 wash

1. TTL does not hold statistics on users' account status beyond 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 \*\*' 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 326

1. 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*

3^ TTL initially indicated this number was 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.

3^ Response to the Notice of Commencement at [9.2.3]. ’\*4 Response to the Notice of Commencement at [9.2.4]. 3^ Response to the Notice of Commencement at [9.2.5]. ’\*6 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.”3*

1. 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.
2. 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.
3. 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].

1. 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.
2. 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.
3. 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.
4. 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.
5. 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)

1. 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* [...]”3\*8 (emphasis added)

328 The Fining Guidelines at 11.

1. 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*

1. 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.
2. 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.
3. 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.”3\*9
4. 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.

1. 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”.
2. 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.
3. 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*

1. 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.”*
2. 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, physicalharm 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.
3. 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 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.

1. 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.
2. 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 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 t'he infringements*

1. 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.
2. 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.
3. 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.
4. 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
   1. **Article 83(2)(b) GDPR: the intentional or negligent character of the infringement**
5. 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* low”.33\*

1. 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

1. 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.
2. 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.
3. 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.*

33° 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*

1. 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.

1. 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.
2. 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.
3. 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.”33’ Therefore, TTL's infringements of Articles 5(1)(c) and 25(1) and (2) GDPR regarding the public-by-default processing was intentional.

1. 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.
   1. Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects
2. 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.
3. 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.
   1. 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
4. 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*

1. 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

33’ 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.

1. 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.
   1. Article 83(2)(e): any relevant previous infringements by the controller or processor
2. No relevant previous infringements arise for consideration in this context.
3. 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
   1. 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
4. 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*

* 1. *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*

* 1. *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*

* 1. *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].

34° Response to the PDD at [9.38]

* 1. *From January 2021, for younger Users aged 16 or 17, the download feature was turned “off”by default.*

*Suggest Your Account to Others*

* 1. *From January 2021, this setting is turned offfor under 16 Users by default.341*

1. 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.
   1. Article 83(2)(g): the categories of personal data affected by the infringement
2. 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.
3. 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.
4. 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.”34*

1. 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.
   1. 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**
2. The infringements became known to the DPC as a result of contact received from the organisations discussed in Section C.1 of this Decision.
3. TTL engaged fully with the DPC from the Notice of Commencement.
4. 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
   1. 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
5. Corrective powers have not previously been ordered against TTL with regard to the subject matter of this Decision.
6. 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
   1. Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42
7. Such considerations do not arise in this case.
   1. 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**
8. 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.
   1. **Decision on Administrative Fine**
9. 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.

1. 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.”*

1. 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:
2. 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.
3. 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.

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Based on the analysis I have set out, I will impose the following administrative fines:
7. 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.
8. 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.
9. 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.
10. 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.
11. 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. 34’*

1. 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. 34’*

1. 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.
2. 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.
3. 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.

34’ 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].











3BB.



TTL wbrnka thac therañ an ”owr•fows“ on diwuaaioø and tlut be P00 file to ex@aTn how Maes of the magnitude proposed are the least onerous meagre available to wh%ve DPC\*s ectlve in cIø•umstences where TIE has already vo imerlĘ implemented changes to addrw the rÆeyarrfi Issues nd te mitigate any theoreficaT risks They may have posed to data subjects. TTS eTso \*tates that I have proœeded to W out t++e owe /sIs en the Tnfrln$œeno largely in g txoad•brush miner that is not t'ompatiMe wnh Anide B4(2} GDPR and the duty to give

regsoø\*, wrhic has made it extremely difficun f'or TTS to m mearńng uT wbmissfoog'^

i ao not acœpt this. rirst, Tnave considered in dezaa ali of the{actors urider Art+câz a3(1) GDeR who \ hue addressed N detNf. This bskn/fañy tbe bese whit regerd to the fed urder 4rtlde 83(2){a}•(k) GOPR. Exter+site raasoninB and errgagemerA has been proyfded In rekrfion to all

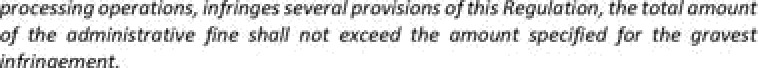
+s'peos of thëse crltezta. X is UmOy not sustalnabN ør Sexually be at O suggest thgt ïnsuffitierA raasoning has bean provl›ded or that it was "impossible“ to understand sha administrative fines have beeu calculated. Indeed, in its ResȚ+anda to the PDD; despite fts c elm, w£ free somhow mene$ed te md very deteged, nuanced gnp •n thy subm\sUœ wlth ragard to all factors, shh has ôeon fdTIy considered.

I am satlsfiaa cbat be Ines.sgedfied would, #Imposed on TTL, be afiló¢tive, prostate and

diswasive, making Into rA #T of the circumstańces oł the Inquiry.

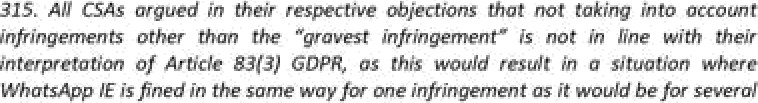
ktav!ng cöm¢eted my asseaWent of 'abedr or rant to Impose e fine{and of the amount of tny au¢h fłna), i rr\*ust no condôat the rsmzdnfng pMsfons OF Artlčla BE GOPR, Oh a uèw to asczrtairăng ń there are any fia-tprs that met reguJre she adjustment rtf the fiw.

Aracle a3(3) GDPR prod tfiat:



I «ate tk t, by „,ay <t EDPB Binding ŒecJslon 0›/zo2\, theE orB rèœr0ed it» assæsme it of the meanźg ąnd ęfføzt.of Article @{3ł GQ9R. Tn Hg t øf the binding nature of that #eós+on and The DP 's [Wfga@ns.of](mailto:Wfga@ns.of) coopetation and «onshtancy N, imar aha, Aródes 6Q1[ and 68 GDOR, It Is rieœszary me to 1óI6uw the EDPB's interpretaôari of Artide B3{2] GDPR.

The rebuaøt passage o£ EOPB BiruJirtg Docsion 0/202s Is as follows:



Response to the PDD at {g.7]•{9.@).

’^ European Data groœztlon Bøard. ’Bnding ezicíon Ç@2\*1 w the d gnrte arJseo nn the draft'de@on of be



*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.*

1. *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.*
2. *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.*
3. *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.*
4. *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.”*
5. *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”.*
6. *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.*
7. *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.*
8. *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 ifa 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.*

1. *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.*
2. *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.*
3. *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.*
4. *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.*
5. 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.
6. 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. 3’*

1. 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.
2. 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.

3’° Response to the PDD at [9.50]-[9.57].

**M.14 Articles 83(4) and (5) GDPR**

1. 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.
2. 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:*

* 1. *the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;*

**

1. 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:*

* 1. *the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;*
  2. *the data subjects' rights pursuant to Articles 12 to 22;*

**

1. 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.*

1. 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/inonced3’1

1. 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,

3’1 Judgment of 23 April 1991, *Hâfner 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.3’\*

1. In the context of Article 83 GDPR, the concept of *“undertoLin9”* 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.
2. 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.3’3
3. 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.3’4
4. 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.3”
5. 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.3’6 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*

3’2 Judgment of 10 September 2009, *Akzo Nobel and Others v Commission,* C-97/08 P, EU:C:2009:536 at [58] — [60].

3’3 Judgment of 14 September 2016, *Ori Martin and SLM v Commission,* C-490/15 P, ECLI:EU:C:2016:678 at [60].

3’4 Judgment of 10 September 2009, *Akzo Nobel and Others v Commission,* C-97/08 P, EU:C:2009:536.

3” Judgment of 8 May 2013, *Eni v Commission,* C-508/11 P, EU:C:2013:289 at [48].

3’6 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 ...3”*

1. 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.
2. 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.
3. 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 6'h Floor, London, EC2Y SEB, England.* {...} .3’8

1. 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.

3’7 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].

3’8 TTL, ‘Director's Report and Financial Statement’ (Year Ending 31 December 2021) at 11.

1. 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.
2. TTL was invited to make submissions in this regard and in its Response to the PDD it did so.
3. 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.3’9
4. 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. 36*

1. 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. 36*

1. 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.*

3’9 Response to the PDD at [9.65]-[9.71].

36° 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*

1. I do not accept TTL's submissions in relation to the above for the following reasons:

 Recital 150 GDPR expressly states that *“iw}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.

1. 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 i...} 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.

1. 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}perationaI independence does not, in* itse//, *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.”3 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.\*6’ 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.\*66 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.

1. 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.

1. 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. Byway of the cover letter accompanying the Final Submissions, TTL confirmed that the estimated turnover for the group of companies headed b B eDance Ltd. for the financial year ending 31 December 2022 was approximately
2. 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

3‘4 Judgment of 11 July 2019, *Huhtamâki Oyj,* T-530/15, EU:T:2019:498 at (228].

3‘s Judgment of 11 July 2013, *Commission v. Stichting Administratiekantoor Portielje,* C-440/11 P, EU:C:2013:514

at [60] and [66].

3‘6 Judgment of the CJEU of 8 May 2013, *Eni v. Commission,* C-508/11, EU:C:2013:289 at [64]-[68]. ”7 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..

1. SUMMARY OF ENVISAGED ACTIONS
2. In summary, the corrective powers that I hereby exercise, by way of this Decision, are as follows:
   1. 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;
   2. I issue a reprimand, pursuant to Article 58(2)(b) GDPR, to TTL regarding the infringements identified in this Decision; and
   3. I impose administrative fines totalling €345 million, as follows:
      1. In respect of TTL's infringement of Articles 5(1)(c) and 25(1) and (2) GDPR **(Finding 1), a** fine of €100 million.
      2. In respect of TTL's infringement of Articles 5(1)(f) and 25(1) **(Finding 3),** a fine of €65 million.
      3. In respect of TTL's infringements of Articles 12(1) and 13(1)(e) **(Finding** 5), a fine of €180 million.
3. 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:
   1. My assessment of the individual circumstances of this particular Inquiry, as summarised earlier in this Decision;
   2. 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);
   3. The requirement for a genuinely deterrent effect, in terms of discouraging both TTL and others from committing the same infringements in the future (dissuasiveness);
   4. 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;
   5. 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 be A o ding to paragraph 333 (a/the Drafi Decision), it affected o i el ild e . 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.”*

* 1. 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 Child Users) were affected by the public-by-default processing in paragraph 333 of the Drafi 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.” \* 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.

* 1. 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 [thej individuals concerned are underage children”. \* 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 SAj 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 characterj, which does not support the imposition of a fine at the upper end of the range proposed by the DPC.” \* 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

’68 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.

* 1. 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* it369.” 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.

1. TTL has the right of an effective remedy as against this Decision, the details of which have been provided separately.

**This Decision is addressed to:**

**TikTok Technology Limited 10 Earlsfort Terrace**

**Dublin 2, Ireland**

**Dated the 1°t day of September 2023**

**Decision-Maker for the Commission:**

*[sent electronically, without signaturej*

Helen Dixon

**Commissioner for Data Protection**

’69 The Final Submissions at [6.26.6].

APPENDIX 1- THE ARTICLE 65 DECISION