CONFUSING BY DESIGN: A Data Protection Law Analysis of TikTok's Privacy Policy

Dr. J. Ausloos & Dr. V. Verdoodt

February 2021

BEUC The European Consumer Organisation

The authors:

Dr. J. Ausloos is a Postdoctoral Researcher at the University of Amsterdam (Institute for Information Law); Research Fellow at the University of Leuven (Centre for IT & IP Law).

Dr. V. Verdoodt is a Postdoctoral Fellow at the London School of Economics; Affiliate Postdoctoral Researcher at Ghent University (Law and Technology; Research Fellow at the University of Leuven (Centre for IT & IP Law).

The opinions expressed in this work reflect the authors' own views and do not necessarily reflect those of the commissioning organisations. The project has been carried out in full compliance with the European Code of Conduct for Research Integrity.

Table of Contents

Executive Summary

TikTok is a short-form video sharing app, centred around a powerful recommendation and personalisation engine and especially popular among young people. This Report comprises a data protection law analysis of TikTok's Privacy Policy and concludes that the company does not comply with the General Data Protection Regulation 2016/679/EU, particularly with regard to the following issues:

MOVING TARGET

Over the past few years TikTok has made an extraordinary number of changes to both its (EU) Privacy Policy as well as its data processing practices, most of which are not publicly documented. This makes hard for interested parties to investigate and bring action accordingly. Improved data protection now, does not excuse for past breaches.

DATA PROTECTION PRINCIPLES

TikTok's Privacy Policy fails to establish compliance with most data protection principles in Article 5 GDPR, significantly weakening data subject rights and invalidating its reliance on the lawful ground in Article 6(1)b GDPR for a number of processing purposes.

CONSENT

TikTok's reliance on consent for personalised advertisement raises significant concerns and fails to comply with the requirements in the GDPR (Articles 4(11), 6(1)a and 7) and ePrivacy Directive (Article 5(3). Neither does the company obtain explicit consent for its processing of special categories of personal data (cf. Article 9 GDPR).

SECURITY & DATA PROTECTION BY DESIGN

TikTok disclaims any responsibility over the security of personal data as it is transmitted on its platform, and anecdotal evidence suggests considerable disregard of the data protection by design requirement in the past, in violation of Articles 5(1)f, 24-25 and 32.

PROTECTION OF CHILDREN

When it comes to the actual processing of personal data, TikTok's Privacy Policy does not appear to differentiate between children and adults. As such, TikTok fails to provide stronger safeguards for children (any person below the age of eighteen) as required by the GDPR (Recitals 38, 71 and Articles 8 and 25 GDPR).

Confusing by Design:

DATA PROTECTION LAW ANALYSIS OF TIKTOK'S EU PRIVACY POLICY[1]

1. A PRIVACY POLICY IN CONSTANT FLUX

Over the past two years, TikTok has repeatedly changed its privacy and data protection policies (and underlying practices). A preliminary assessment of the company's compliance with the General Data Protection Regulation (GDPR), carried out in the fall of 2019, brought to light grave GDPR violations (e.g. relating to users without an account, age verification and personalised advertising).[2] Between that first analysis and the time the analysis in this Report was done, there have been at least three different versions of TikTok's privacy and data protection (and cookie) policies, with significant differences between them. These differences relate to the geographic scope, language and content of the policies. In the absence of any clear information on TikTok's own website as to these frequent changes, one has to resort to self-archiving or external tools such as web.archive.org, to verify all of the policy reincarnations.[3] Meanwhile, TikTok has also made changes to its technical infrastructure and user interface affecting their compliance with the GDPR. These changes and when they were made, are harder to independently verify in retrospect. That said, it can be expected that the numerous investigations initiated by data protection authorities over the past two years may bring to light problematic practices in the past[4].

[1] The analysis in this report is based on accessing and observing TikTok's Privacy Policy via an iPhone X (iOS 14) and a MacBook Air (OS11) from a Dutch IP address

[2] This Report is available upon request via digital@beuc.eu

[3] https://web.archive.org/web/*/https://www.tiktok.com/legal/privacy-policy. Note: the actual URL for TikTok's privacy policies has changed over the years, making it even harder to identify all relevant policies through web archiving tools.

[4] UK ICO investigating TikTok for handling of UK children's data (July 2019) ; Dutch data protection authority to investigate TikTok (May 2020); The Danish data protection authority ('Datatilsynet') announced that it had launched an investigation into TikTok (June 2020); The EDPB establishes a Task Force on TikTok (June 2020); The Italian data protection authority initiates proceedings against TikTok (December 2020) and imposes limitation on processing operations (January 2021).

Summary-overview of recorded changes of privacy/data protection policies (applicable in the EU)[5] starting with the one available on 1 January 2019:

	Available official EU languages	Selection of key changes compared to previous policy
August 2018	EN	
January 2019	EN	Contact details; removal of specific list of countries where personal data was processed;[6] creation of separate cookie policy; details on use of location data
October 2019	DE; EN; ES; FR; IT; PT	More details on personal data that is collected, processing purposes and categories of third parties whom personal data is shared with; changed some of the lawful grounds relied on for some processing purposes;[7] explicit reference to standard contractual clauses as ground for data transfers; removal of mention that data subjects have a right to take legal action in relation to any breach of their rights
July 2020	DE; EN; ES; FR; IT ; NL ; PT ; SE	Relevant controller established in Ireland; dedicated summary for 13-18 year olds; addition of two more lawful grounds;[8] more detailed list of purposes under 'legitimate interests' ground and recognition of balancing test;[9] details on procedure after deleting account

Put briefly, TikTok regularly updates its Privacy Policy, the latest revision to its English language EU-wide Privacy Policy dating back to July 2020 at the time of writing.[10] While in principle, it is commendable for controllers to update their policies to adequately reflect their practices, such updates should be done in a thoughtful manner. Currently, TikTok does not have an archive of its previous privacy policies, nor does it list the (main) changes that have occurred. Moreover, TikTok will only notify users when there are 'material' changes to the policy, which remains entirely at the discretion of the company to decide. As a result, **it is hard to analyse TikTok's data practices and compliance over time.** Moreover, it should be emphasised that improvements over time do not excuse breaches of data protection rules in previous policies and practices.[11]

[5] Privacy policies from before this date can still be accessed via https://web.archive.org. The many changes to privacy policies applicable in other jurisdictions will not be discussed here.

[6] In particular: 'The personal data that we collect from you may will be transferred to, and stored at, a destination outside of your country and the European Economic Area ("EEA~~"), specifically to the United States of America, Singapore, Japan or to China. We transfer your information to the servers of our hosting providers in Japan, and in the United States of America."). Further information regarding the transfer of data outside of the EEA is available~~. *Please contact us at privacy@tiktok.com if you have any questions*'. [Note: ~~Removed~~ and *Added*]

[7] E.g. 'detect abuse, fraud and illegal activity on the Platform' changed from lawful ground in Article 6(1)b to Article 6(1)c GDPR.

[8] Article 6(1)d and e GDPR.

[9] This will further be detailed in Sections 2 and 3.

[10] The EEA, UK, Swiss Privacy Policy from July 2020 will be the reference point throughout the rest of this Report. It was last accessed on 2 February 2021.

[11] See similarly: Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (11 April 2018) para 31.

> We will notify all users of any material changes to this policy through a notice on our Platform or by other means. We update the "Last Updated" date at the top of this policy, which reflects the effective date of the policy. By accessing or using the Platform, you acknowledge that you have read this policy and that you understand your rights in relation to your personal data and how we will collect, use and process it. For more information, click here.

Excerpt 1 – 'How will we notify you of any changes to this Privacy Policy?'

TikTok's current Privacy Policy also raises questions from the perspective of the fairness and transparency principles.[12] For instance, all three different policies (US, EEA + Switzerland, and rest of the world) are confusingly located on the same webpage, one after the other. When clicking the hyperlink to the EU Privacy Policy, users are simply referred to the location on the webpage where that policy starts. This webpage ends with a section 'Supplemental Terms – Jurisdiction-Specific', that includes dedicated specifications for a number of jurisdictions.[13] TikTok only offers privacy policies in nine EU official languages (English, French, Dutch, German, Italian, Polish, Portuguese Swedish and Spanish).[14] While the language can be changed when accessing through a web-browser,[15] this is not possible when accessing the Privacy Policy (or any other policy) within the TikTok app itself. These accessibility issues, especially for users who do not understand the default language, are problematic from the perspective of different legal regimes (notably data protection and consumer law).

2. Data Protection Principles

Article 5 GDPR lays down the key data protection principles.[16] Crucially, every processing operation needs to be *lawful, fair and transparent* (Art.5(1)a). The *purpose limitation* principle requires that personal data only be collected for specific, explicit and legitimate purposes.[17] The *data minimisation* principle, in turn, requires that that personal data is adequate, relevant and limited to what is necessary for achieving those purposes.[18] The *storage limitation* principle, finally, requires that personal data can in principle only be stored for as long as it is necessary for the purposes that it was collected for.[19]

2.1. Purpose Limitation and Data Minimisation

Personal data can only be lawfully processed if and to the extent one of the six grounds in Article 6(1) applies (see below, Section 3). Each lawful ground inherently relates to a specific,

[12] Article 5(1)a GDPR.
[13] Notably, India, Indonesia, Japan, South Korea, and the United Arab Emirates.
[14] The Swedish version of TikTok's Privacy Policy only became available in December 2020, without an apparent announcement.
[15] Drop-down menu at the bottom of the webpage.
[16] Cf. Article 8(2) Charter of Fundamental Rights of the EU, requiring 'data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.'
[17] Article 5(1)b GDPR.
[18] Article 5(1)c GDPR.
[19] Article 5(1)e GDPR.

explicit and legitimate processing purpose. Put differently, personal data needs to be necessary for a processing operation, which needs to be necessary for a specific processing purpose, which in turn requires a specific lawful ground (cf. Figure 1). Concretely, this means that personal data can be processed in a number of different ways, for potentially different purposes.[20] In any case, each individual purpose pursued by the controller will need a dedicated lawful ground.

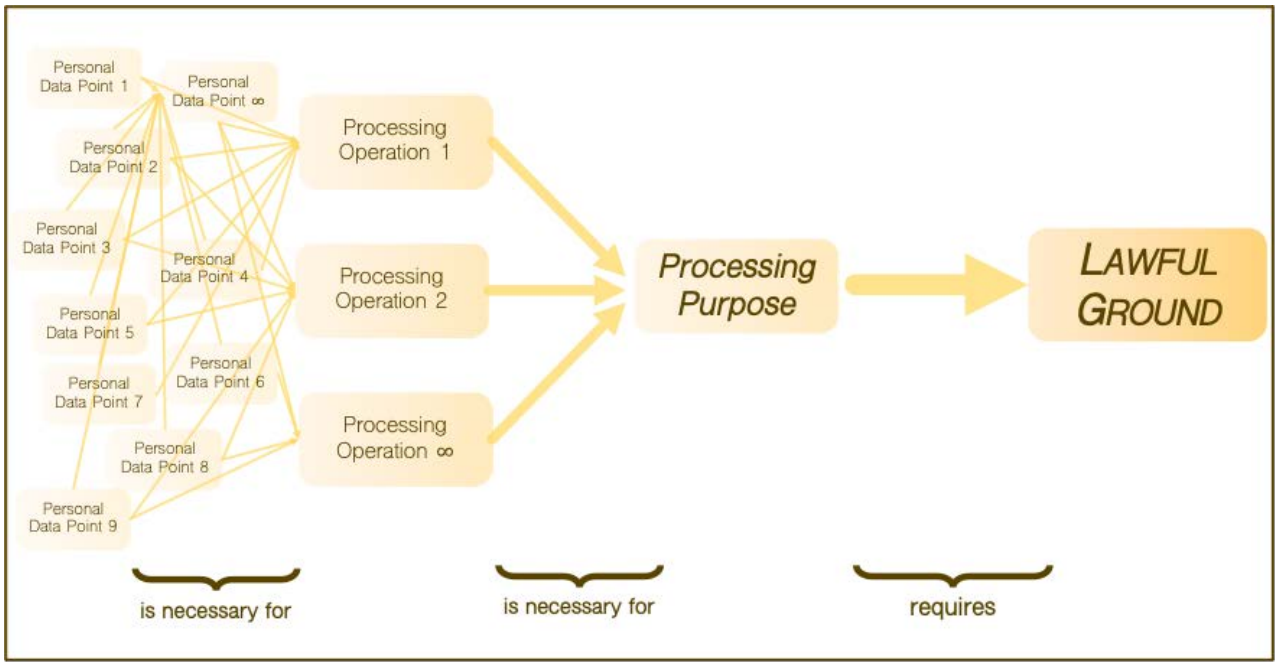

Figure 1 - Relationship between personal data, processing, purposes and lawfulness

TikTok's Privacy Policy lists many personal data points, processing operations, processing purposes and lawful grounds. Occasionally, the policy explains what purposes specific personal data will be processed for, yet it fails to do so in a systematic and exclusive manner (e.g., personal data A, B and C will be processed *exclusively* for purposes X and Y). Similarly, for each lawful ground[21] it relies on, a number of processing purposes are listed, without making clear what personal data feeds into what specific purpose. As a result, TikTok fails to clearly and consistently connect each personal data point with a specific processing operation, with a specific processing purpose, with a specific lawful ground. This is problematic not just from a theoretical perspective, but has very concrete implications for effective and complete protection of data subjects. Notably, because it prevents a proper evaluation of GDPR compliance[22] as well as significantly thwarts the effectiveness of data subject rights.

[20] As a matter of fact, 'personal data' points are virtually limitless in number, constantly morphing and interacting with one another.

[21] Cf. Article 6(1) GDPR.

[22] In breach of the overarching fairness, transparency and accountability principles. See notably: Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 13).

2.1.1. *Inability to meaningfully verify compliance*

TikTok's failure as described above, essentially makes it **impossible to properly evaluate the company's compliance with the GDPR.** Indeed, without TikTok indicating the exact and sole purposes that each personal data (category) is processed for, readers cannot assess whether the personal data is 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed',[23] nor whether they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which' they are processed.[24] The Policy can create the impression that *all* personal data listed is – or at least can be – processed for all specified purposes.

An interesting illustration can be found in personal data TikTok collects from people who do not have an account. The text below (Excerpt 2) gives a sample of how much personal data is collected, even from users who chose *not* to create a TikTok account. Even though the different types of personal data being collected are quite specific, the excerpt also illustrates how it is unclear what all of this personal data will be used for exactly (and on what lawful ground it will be processed).

> **Technical Information we collect about you.** We collect certain information from you when you use the Platform including when you are using the app without an account. Such information includes your IP address, instance IDs (which allow us to determine which devices to deliver messages to), mobile carrier, time zone settings, identifier for advertising purposes and the version of the app you are using. We will also collect information regarding the device you are using to access the Platform such as the model of your device, the device system, network type, device ID, your screen resolution and operating system, audio settings and connected audio devices. Where you log-in from multiple devices, we will be able to use your profile information to identify your activity across devices.

Excerpt 2 - Some of the personal data TikTok collects from users, including those without an account[25]

2.1.2. *Inability to meaningfully exercise data subject rights*

The fact that **it is not clear *what* personal data is collected for what purposes under what lawful ground exactly**, is problematic because it affects data subjects' ability to invoke their rights. Notably, the applicability in any given case of the rights to data portability,[26] to object,[27] and to erasure[28] will depend on the lawful ground relied on for processing the respective personal data. In particular, the *right to data portability* only applies to a specific subset of personal data (i.e., data which the data subject has provided to the controller itself), processed on the basis of consent[29] or contract performance.[30] The *right to object* only

[23] Article 5(1)c GDPR.
[24] Article 5(1)e GDPR.
[25] Not long ago, TikTok allowed anyone to use TikTok without creating an account. However, in 2020 TikTok appears to have made it impossible to use the smartphone app without an account (it is unclear when exactly TikTok made this change). Yet, at the time of writing, people without an account can still freely access TikTok through a web-browser (on mobile and desktop devices).
[26] Article 20 GDPR.
[27] Article 21 GDPR.
[28] Article 17 GDPR.
[29] Articles 6(1)a or 9(2) GDPR.
[30] Article 6(1)b GDPR. Article 29 Working Party, 'Guidelines on the Right to Data Portability' (Guidelines, 5 April 2017).

applies to specific processing operations that rely on one of the last two lawful grounds under Article 6 GDPR.[31] And, finally, each of the six situations in which the *right to erasure* can be invoked[32] im-/explicitly hinges on what lawful ground is relied on. Put differently, without knowing the specific purpose(s) and corresponding lawful ground, data subjects cannot effectively exercise their right to erasure with regard to specific personal data points listed in TikTok's Privacy Policy. With this in mind, the tools and options for erasing personal data that TikTok explicitly offers to users now are insufficient.[33] In short, because it does not make clear *what* ground it relies on for processing what personal data, **TikTok effectively renders it difficult for data subjects to exercise their rights.**

The Privacy Policy also fails to clarify what data subject rights are expected to be refused and under what circumstances, a duty on controllers' shoulders pursuant to Articles 13-14 and 25 GDPR.[34] For example, it is unclear to what extent data subjects can successfully exercise their *right to object* with regard to any of the processing purposes TikTok lists under the last lawful ground (see (f) in Table 1). *A priori*, data subjects have a right to object vis-à-vis any processing operation for purposes that fall under the legitimate interests ground (f). While the Privacy Policy recognises that TikTok conducts a balancing test with regard to the processing operations under Article 6(1)f, it **fails to state that data subjects have a right to challenge that balance through the right to object**[35] (see Excerpt 3).

Relatedly, the Privacy Policy only recognises it takes into account users' privacy rights in said balancing act, despite the GDPR requiring them to take into account all other rights, freedoms and interests at stake, not just of its users but also others. For example, TikTok should explicitly consider potential privacy-violations of *non*-users featuring in videos, as well as potential censorship and discrimination of users that are posting 'controversial' or 'ugly' content.[36] These are equally important elements to consider in a balancing act under the

[31] I.e. Article 6(1)e GDPR: necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; Article 6(1)f GDPR: legitimate interests.
[32] Article 17(1) GDPR.
[33] Users can, for example, choose to delete specific videos they posted or delete their account altogether. There are no apparent tools however, for requesting erasure in a more granular manner with regard to all personal data listed in TikTok's Privacy Policy.
[34] Recital 59 GDPR. Also see: Jef Ausloos and others, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 jipitec, 307–08.
[35] Article 21(1) GDPR.
[36] Late 2019, it was reported that TikTok downranks videos from people with disabilities as well as queer and overweight people, regardless of the actual content they post. This practice is said to protect individuals who are 'susceptible to harassment or cyberbullying based on their physical or mental condition'. Concretely, when identified, these videos were marked to be only visible within the country where uploaded. When reaching a certain number of views, videos from 'particularly vulnerable users' were automatically pushed in the 'not recommended' category, so that they could no longer feature in the 'For You Feed'. These measures were criticised for being patronising, punishing potential victims instead of trolls. Soon after, other stories broke that TikTok was also preventing 'ugly content' (including 'abnormal body shapes' and 'ugly facial looks') from appearing in the central 'For You Feed', because it would make videos 'much less attractive', fail to retain new users and grow the app.
See, *inter alia*: Chris Köver, 'Discrimination - TikTok curbed reach for people with disabilities' (*netzpolitik.org*, 12 February 2019) <https://netzpolitik.org/2019/discrimination-tiktok-curbed-reach-for-people-with-disabilities/> accessed 16 September 2020; Sam Biddle and Paulo Victor Ribeiro, 'Invisible Censorship. TikTok Told Moderators: Suppress Posts by the "Ugly" and Poor' (*The Intercept*, 16 March 2020) <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/> accessed 20 January 2021.

legitimate interests ground[37] and challenges through the right to object.[38] Finally, the Privacy Policy also claims only to consider TikTok's own business purpose in the balancing act (see Excerpt 3). Yet, the GDPR's preparatory works,[39] CJEU case law,[40] as well as the European Data Protection Board and European Data Protection Supervisor (EDPB/S) guidance,[41] all suggest that business interests alone are unlikely to be able to override data subjects' rights, freedoms and interests.[42]

> Where we process your information to fulfill our legitimate interests, we conduct a balancing test to check that using personal data is really necessary for us to achieve our business purpose. When we carry out this balancing test we also take into account the privacy rights of our users and put in place appropriate safeguards to protect their personal data.

Excerpt 3 - TikTok's balancing under Article 6(1)f GDPR

2.2. Lawful, Fair and Transparent processing

Under the third heading in TikTok's Privacy Policy, the company refers to all six lawful grounds for processing.[43] For each of these lawful grounds, a number of processing purposes are specified (see Table 1).

Art. 6(1)	We will use the information we collect about you based on the legal grounds described below:	
a	With your **consent**, we will use your information to	(1) provide you with **personalised advertising**. Please see the sections on Advertisers in "Information from Third Parties" for more information. You can control your personalised advertising settings at any time via your app settings. Please go to 'Privacy and safety' and then 'Personalization and data' to manage and control your advertising preferences. If you do not consent to personalised advertising, you will still see non-personalised advertising on the Platform.

[37] Article 6(1)f GDPR.
[38] Article 21(1) GDPR.
[39] Cf. data subject rights 'could limit to a certain extent freedom to conduct business. However, such limitation does not seem disproportionate, taking account the positive impacts.' European Commission, 'Commission Staff Working Paper: Impact Assessment Accompanying the Proposals for General Data Protection Regulation and Directive on Data Protection in Police and Judicial Matters' (Commission Staff working Paper, 25 January 2012) 129 Annex 7.
[40] Most notably in: Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317 [99]; Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772 [45]; *GC and Others v CNIL C-136/17*, Judgment of24 September 2019 C-136/17, para 53.
[41] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (2 April 2013) 46; European Data Protection Supervisor, 'Preliminary EDPS Opinion on the Review of the EPrivacy Directive (2002/58/EC)' (Opinion, 22 July 2016) 14–16; European Data Protection Supervisor, 'Opinion on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (Opinion, 14 March 2017) 7 et seq.
[42] See in detail: Jef Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (Oxford University Press 2020) 333–49; Hielke Hijmans, *The European Union as Guardian of Internet Privacy : The Story of Art 16 TFEU* (Law, Governance and Technology Series 31, Springer 2016) 196, 216–17, 258; Ausloos and others (n 36) 306–07.
[43] As listed in Article 6(1) GDPR.

b	In accordance with, and to perform our **contract** with you, we will use your information to	(2) **provide the Platform** and associated services
		(3) **notify you** about changes to our service;
		(4) provide you with **user support**;
		(5) **enforce our terms**, conditions and policies;
		(6) **administer the Platform** including troubleshooting;
		(7) **personalise the content** you receive and provide you with tailored content that will be of interest to you;
		(8) enable you to **share** User Content and **interact** with other users;
		(9) enable our **messenger** service to function if you choose to use it and are 16 or above;
		(10) enable you to participate in the **virtual items program**; and
		(11) **communicate** with you.
c-e	In order to comply with our **legal obligations** and **as necessary to perform tasks in the public interest or to protect the vital interests**	(12) we use your data to help us prevent and respond **to abuse, fraud, illegal activity** and other potentially harmful content on the Platform
f	In accordance with our **legitimate interests** to provide an effective and dynamic Platform, we may use your information to:	(13) ensure your **safety and security**, including reviewing User Content, messages and associated metadata for breaches of our Community Guidelines and our Terms of Service;
		(14) ensure content is presented in the most effective manner for you and your device;
		(15) **understand how people use the Platform** so that we can improve, promote and develop it;
		(16) **promote** popular topics, hashtags and campaigns on the Platform;
		(17) **carry out data analysis** and test the Platform to ensure its stability and security;
		(18) **verify your identity**, for example, to enable you to have a 'verified account', and your age, for example, to ensure you are old enough to use certain features;
		(19) **provide non-personalised advertising**, which keeps many of our services free;
		(20) **infer your interests for optimising our advertising** offerings, which, where you've consented to personalised advertising, may be based on the information our advertising partners provide to us;

		(21) measure the effectiveness of the advertising you see on our Platform;
		(22) inform our algorithms so we can deliver the most relevant content to you and to prevent crime and misuse of the Platform;
		(23) **carry out surveys** regarding our services, products and features;
		(24) allow you to participate in **interactive features** of the Platform; and
		(25) enable you to **socialise on the Platform**. For example, we may allow other users to identify you via the "Find Friends" function or through their phone contacts or connect you with other users by tracking who you share links with.

Table 1 - Overview of lawful grounds relied on in Section 3 of TikTok's Privacy Policy (emphasis added)

While this detailed list appears quite comprehensive, there are still a number of open issues. *Firstly*, as already elaborated in the previous paragraphs, **the Privacy Policy fails to specify what specific personal data** (processing operation) **feeds into** each and every one of these **individual processing purposes**. *Secondly*, there seems to be some overlap between different processing purposes that rely on different grounds.[44] This is especially true for the group of processing purposes under (12), for which it is unclear what specific ground will be relied on in any given case. Moreover, the list of purposes appears to include different levels of purposes with generic/overarching purposes (e.g., (2), (6)) and more specific ones (e.g., (8), (18)). This is problematic as it implies **TikTok can rely on different lawful grounds to justify the same processing purposes (and underlying processing operations)**. A processing purpose such as (2) 'provide the Platform and associated services' is not specific enough 'to allow that compliance with the law can be assessed and data protection safeguards applied'[45] and unlikely to be able to rely on the second lawful ground as interpreted by the EDPB.[46] *Thirdly*, **combining the processing purposes under (12), and especially grouping together the alleged lawful grounds they rely on, is of questionable validity**. Indeed, the vital interests ground[47] can only be relied on when the respective processing of personal data is 'necessary to protect an interest which is essential for the life of the data subject or that of another natural person.'[48] Similarly, the ground 'necessary for

[44] E.g. (2), (6), (8), (9) and (25); or: (2), (6), (7), (14), (16) and (22).
[45] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (2 April 2013) 15–16; European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subject v2.0' (8 October 2019) 6–7.
[46] European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjectq' (8 October 2019).
[47] Article 6(1)d GDPR
[48] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (Guidelines, 6 February 2018) 14. Elsewhere, the Article 29 Working Party stated that 'the phrase 'vital interest' appears to limit the application of this ground to questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject (or in case of Article 8(2)(c) also of another person)' and 'a restrictive interpretation must be given to this provision'. See: Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (Opinion, 9 April 2014) 20–21.

the performance of a task in the public interest'[49] begets a very narrow interpretation, generally only covering situations where the public task has been explicitly 'attributed in statutory laws or other legal regulations' or they are enlisted 'to cooperate with law enforcement authorities, for instance in the fight against fraud or illegal content on the Internet'.[50]

2.3. Storage Limitation

Personal data can in principle only be stored for as long as 'is necessary for the purposes for which the personal data are processed' (storage limitation principle)[51]. Controllers are required to inform data subjects about 'the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period'[52] and keep a record of 'the envisaged time limits for erasure of the different categories of data',[53] where possible. The Article 29 Working Party[54] explained that the information given to data subjects should allow them to 'assess, on the basis of his or her own situation, what the retention period will be for specific data/purposes'.[55] Indeed, 'it is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.'[56] In light of how vague TikTok's Privacy Policy is about the actual retention (cf. *Excerpt 4*), let alone distinguish between different categories of data, it **is doubtful whether TikTok complies with these information obligations**. As a consequence, it is also **impossible to adequately verify TikTok's compliance** with its obligations under the purpose limitation, data minimisation and storage limitation principles,[57] combined with the provisions on responsibility and data protection by design and default (see below, Section 4).[58]

> We retain your information for as long as it is necessary to provide you with the service so that we can fulfil our contractual obligations and exercise our rights in relation to the information involved. Where we do not need your information in order to provide the service to you, we retain it only for so long as we have a legitimate business purpose in keeping such data. [...] In each case, there are also occasions where we may need to keep your data for longer in accordance with our legal obligations or where it is necessary for legal claims.

Excerpt 4 - 'How long we keep your personal data'

[49] Article 6(1)e GDPR
[50] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (n 50) 21–22. One could think of reporting duties under future rules on content moderation, for example.
[51] Article 5(1)e GDPR.
[52] Articles 13(2)a; 14(2)a GDPR.
[53] Article 32(1)f GDPR.
[54] Now 'European Data Protection Board' or EDPB.
[55] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 13) 38.
[56] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 13) 38.
[57] Article 5(1)b, c and e GDPR.
[58] Articles 24-25 GDPR.

3. (Un)Lawful Processing of Personal Data

3.1. Consent for Targeted Advertising

3.1.1. Specific and informed

TikTok's Privacy Policy explicitly states it relies on consent as a lawful ground[59] for processing personal data in order to provide personalised advertisement (see Table 1). Yet it is unclear, from the Policy, what exactly this consent relates to in particular. More specifically, the way in which the 'inference of interests'[60] and 'personalised advertising'[61] processing purposes are formulated, allows TikTok to only consider consent to relate to the *delivery* of personalised advertisement. In other words, the actual commercial profiling underlying the personalisation appears not to fall under this processing purpose, and hence cannot be halted by data subjects withdrawing their consent. This framing can be considered to mislead data subjects about the effect of withdrawing consent (or not consenting in the first place) will have on how their personal data is processed.

> We infer your interests, gender and age for the purpose of personalising content. We also infer the interests of our users to better optimise advertising across our Platform. If you have consented, we will use this information for the purpose of serving personalised advertising.

Excerpt 5 - User Consent and Behavioural Information used by TikTok

At this stage, it is also worth referring to the consent notice that is presented to new users upon opening the app for the first time (cf. Figure 2). The way in which the consent notice is framed can be considered to nudge new users to select 'Accept' in order to be able to use the app[62]. There is not a comparable 'decline' button. Additionally, the information given within the notice is insufficient in light of what the GDPR requires.[63] The consent notice simply states the user will allow 'TikTok to personalize the ads you see based on your activity on the app and data received from third parties'. Only if users click on 'Manage in settings' they will be able to see, for example, that ads are personalised on the basis of activity 'on and off' TikTok. Also, just by reading the notice, users are not able to assess exactly what personal data might be processed and from which third parties it might originate. Moreover, by clicking 'Accept' users consent to the personalisation of ads on the basis of app activity *and* on the basis of data received from third parties in a bundled manner. Whereas, by clicking on 'Manage in settings'

[59] Article 6(1)a GDPR.
[60] See Excerpt 5.
[61] See (1) in Table 1.
[62] Forbrukerrådet, *Deceived by Design (June 2018)* https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
[63] Articles 4(11), 6(1)a and 7 GDPR.

TikTok does provide the possibility (not) to consent to these two data processing operations separately. Another source of concern is that when users do make the effort to manage their settings, switching on 'Personalized ads' automatically switches on 'Ads based on data received from partners' as well. This means consent is bundled yet again, meaning that consenting to personalised ads appears to imply consenting 'by default' to those ads being based on data received from unspecified TikTok partners ("*advertisers and other partners*").

In light of the above, TikTok's Privacy Policy and consent notice arguably fail to comply with the requirement for consent to be specific[64] and informed,[65] as well as the broader fairness and transparency principles.[66]

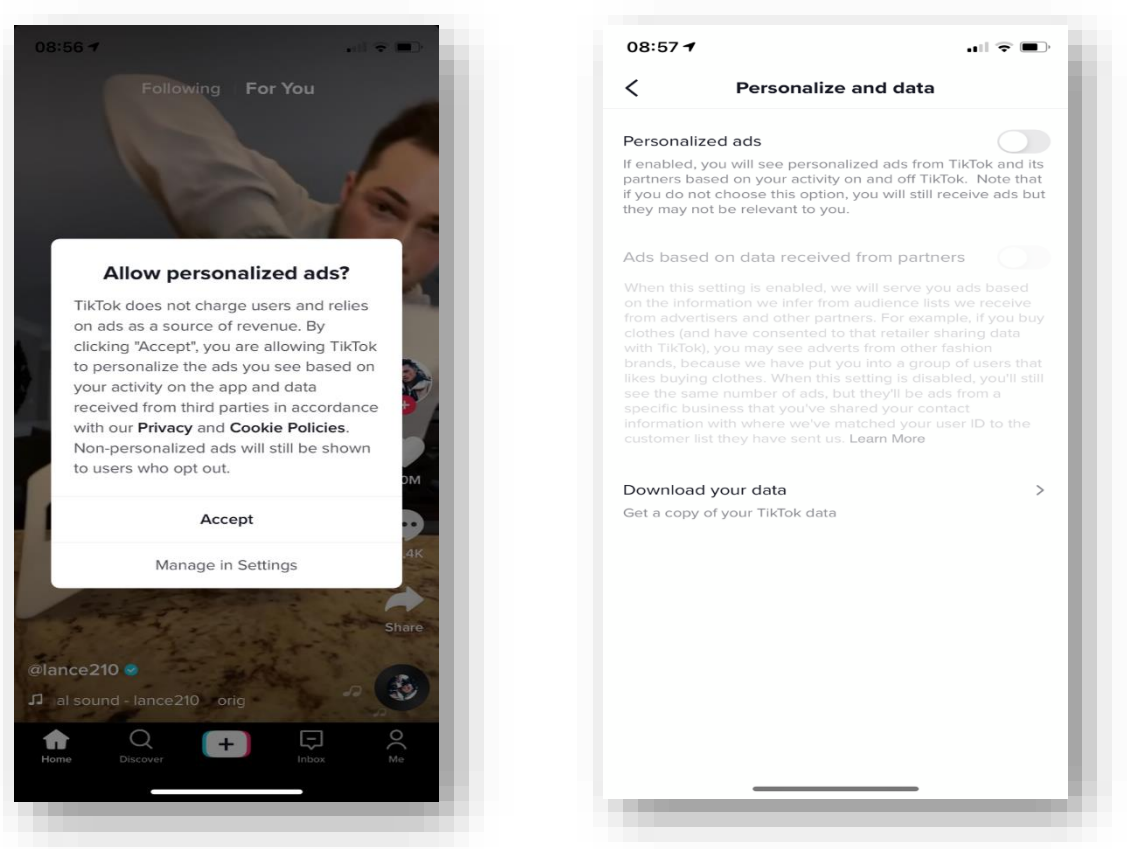

Figure 2 - Consent notice presented to first time users on iOS[67].

[64] Failing the requirement of granularity in consent requests. See: European Data Protection Board *Guidelines on consent under Regulation 2016/679* 05/2020, at 12–14 (European Union 2020).
[65] Cf. Article 4(11) GDPR. See notably: (n 68).
[66] Article 5(1)a GDPR. See notably: Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 13); Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130.
[67] On Android the pop-up's design highlights 'Accept' in red, nudging consumers even more strongly to activate personalised ads. See Appcensus, *TikTok App Analysis Report* (2021). Report available upon request from digital@beuc.eu.

3.1.2. Consent under the ePrivacy directive

At this stage, it is also worth briefly referring to the Article 5(3) in the ePrivacy Directive,[68] that requires controllers to obtain users' consent before 'the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user'. Such prior consent is *not* required only when technical storage or access to the respective information takes place 'for the sole purpose of carrying out the transmission of a communication over an electronic communications network' or 'as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'. It should be emphasised that the latter exception should be interpreted narrowly.[69]

A number of data-categories listed in TikTok's Privacy Policy appear to fall within the scope of Art.5(3) ePrivacy Directive, notably under 'Technical Information we collect about you' (see above, Excerpt 2). Moreover, the Privacy Policy fails to detail what specific purposes these data points will be processed for exactly (see above), despite Art.5(3) ePrivacy Directive requiring it to provide 'clear and comprehensive information [...] about the purposes of the processing.' TikTok does give more details on its use of cookies (and other tracking technologies) in a separate 'Web Cookies Policy'.[70] But this policy *only* covers situations where people visit their website on the tiktok.com domain, and does not apply to any of TikTok's 'services, applications, products and content'.[71] As a result, one can only conclude that **TikTok fails to comply with its requirements pursuant to Article 5(3) ePrivacy Directive.** It should also be emphasised that breaches of (national implementations of) the ePrivacy Directive do fall within the enforcement competences of national data protection authorities.[72] This was recently validated by the French CNIL, issuing 35 million and 100 million fines to Amazon and Google respectively, for breaching consent and transparency requirements in their cookie practices.[73]

[68] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[69] Article 29 Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (7 June 2012).

[70] https://www.tiktok.com/legal/tiktok-website-cookies-policy?lang=en, accessed 21 January 2021.

[71] Even within this limited context, TikTok appears to violate the requirement that consent shall be as easy to withdraw as it is to give (Article 7(3) GDPR). After all, consent is asked through a popup cookie-banner when first visiting TikTok.com in a big colourful button. Refusing to consent requires people to click on the colourless button 'Cookie Policy' > scroll to nearly the end of the policy > click on 'Open cookie settings' > manually opt out of each third party tracking cookies individually. Withdrawing consent to the placement of these cookies *after* it has been given requires people to first find the greyed out text with legal information > click 'More' > click 'TikTok.com Cookies Policy' > click on 'Open cookie settings' > manually opt out of each third party tracking cookies individually. In short, consenting only requires the click of one very visible button on TikTok.com's landing page, while withdrawing consent requires a series of steps.

[72] I.e. they do not have to go through the so-called 'one-stop-shop mechanism' (Cf. Articles 4(23), 55-56, 60-70 and Recitals (124) (140) of the GDPR). See also: Article 29 Working Party, 'Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority' (Guidelines, 5 April 2017).

[73] CNIL, 'Cookies : Sanction de 35 Millions d'euros à l'encontre d'AMAZON EUROPE CORE' (10 December 2020) <https://www.cnil.fr/fr/cookies-sanction-de-35-millions-deuros-lencontre-damazon-europe-core> accessed 30 January 2021; CNIL, 'Cookies : Sanction de 60 Millions d'euros à l'encontre de GOOGLE LLC et de 40 Millions d'euros à l'encontre de GOOGLE IRELAND LIMITED' (10 December 2020) <https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-google-llc-et-de-40-millions-deuros-lencontre-de> accessed 30 January 2021.

3.1.3. *Explicit consent for processing special categories of personal data*

Finally, it should be pointed out that TikTok's Privacy Policy is silent about the processing of 'special categories of personal data'.[74] The GDPR installs a general ban on processing this category of personal data, unless one of the exceptions applies.[75] Only two of these exceptions appear to be relevant for the bulk of TikTok's processing operations, i.e. (a) explicit consent to processing specified purpose(s), or (e) processing relates to personal data which are manifestly made public by the data subject. Importantly, these exceptions do not replace, but come on top of, the requirement to have a lawful ground.[76] Oftentimes user generated content that is posted on TikTok will contain some special categories of personal data. To the extent that content is posted *publicly,* one could consider TikTok can process the respective special categories of personal data pursuant to the second exception.[77] When special categories of personal data appear from content that is posted on a private account or features in private messages, or when they are inferred from other personal data, explicit consent[78] will generally be the only realistic option to legitimately process said personal data. It appears that TikTok does indeed process special categories of personal data, notably in the context of content moderation practices. For example, investigative research has demonstrated how TikTok's content moderation is affected by, for example, the political nature of content,[79] or certain health-related information[80].[81] It is unclear to what extent TikTok is also processing 'special categories of personal data' for other purposes than content moderation. In any case, in the absence of any specific information on the processing of 'special categories of personal data' in the Privacy Policy, at least regarding content moderation, **TikTok appears to breach its duties under Article 9 GDPR.**

3.2. Necessary for the performance of a contract

As apparent from Table 1, TikTok lists ten processing purposes it claims to be necessary to 'perform the contract' with its users, implying reliance on the second ground for lawful processing in the GDPR. The second lawful ground relates to processing operations that are necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract. This ground has traditionally been interpreted very restrictively.[82] The European Data Protection Board (and Working Party 29 before that) repeatedly emphasised that this lawful ground requires 'a direct and objective link between the processing of the data and the purpose of the execution of

[74] Defined in Article 9(1) GDPR as: 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.
[75] Listed in Article 9(2) GDPR.
[76] Pursuant to Article 6(1) GDPR.
[77] Article 9(2)e GDPR.
[78] Article 9(2)a GDPR.
[79] Markus Reuter and Chris Köver, 'TikTok - Cheerfulness and censorship' (*netzpolitik.org*, 23 November 2019) <https://netzpolitik.org/2019/cheerfulness-and-censorship/> accessed 23 January 2021.
[80] Köver (n 38).
[81] Biddle and Ribeiro (n 38).
[82] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (n 50) 16–18.

the contract',[83] not to mention that the contract itself needs to be valid under relevant contract laws.[84] Determining the necessity entails a fact-based 'least intrusive means' test in light of the rationale of the contract itself.[85] Indeed, terms that are unilaterally imposed on data subjects within the contract, are not automatically necessary for its performance.[86] It is important to stress these points as reliance on this second lawful ground has considerable consequences for data subject rights. For instance, it will be a lot harder or even impossible to meaningfully exercise the right to erasure[87] and to object.[88] Moreover, the withdrawal of consent will not be available either. The only way to resist the respective processing operations will therefore often be to stop using the service altogether.[89]

The uncertainty as to the scope of the second lawful ground has also led the EDPB to adopt interpretation Guidelines in October 2019. Put very briefly, it confirms the very narrow scope of the ground, and the need for controllers to be able to demonstrate that '(a) a contract exists, (b) the contract is valid pursuant to applicable national contract laws, and (c) that the processing is objectively necessary for the performance of the contract'.[90] Importantly, when assessing the rationale of the contract itself, one needs to consider the position of both controller *and* data subjects. In other words, can the contract still be considered 'performed' in the eyes of a reasonable data subject, when the respective processing operation does not take place?[91] This implies a complex assessment of user expectations, requiring more field research.[92]

[83] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (10 April 2018) 8.
[84] See BEUC Report, (2021), *TikTok without Filters*, Section 4.
[85] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (n 50) 17; European Data Protection Board (n 48) 7; Joined Cases Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C:2010:662; *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* ECLI:EU:C:2017:336, para 30 (2017).
[86] 'For example, Article 7(b) [now Article 6(1)b GDPR] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.' Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (n 50) 16–17.
[87] Essentially only invokable when it can be established that the lawful ground is not valid *in casu*, there is a legal obligation to erase, or the contract itself is rescinded).
[88] Only available with regard to processing operations that rely on either of the last two lawful grounds.
[89] European Data Protection Board (n 48) 11.
[90] European Data Protection Board (n 48) 9.
[91] European Data Protection Board (n 48) 10.
It is also useful to refer to the proposed *Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC of 2020* European Commission COM(2020) 825 final, European Commission (European Union European Commission 2020). (DSA). In its current form, Article 29(1) would require very large online platforms that use recommender systems to offer 'at least one option which is not based on profiling, within the meaning of Article 4(4)' of the GDPR. Even if it is only a proposal at this stage, it does indicate the European Commission's thinking in this regard.
[92] The EDPB formulated guiding questions to help assess the applicability of the second lawful ground:
'What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?
What is the exact rationale of the contract (i.e. its substance and fundamental object)?
What are the essential elements of the contract?

With this in mind, it is now possible to take a closer look at TikTok's Privacy Policy in particular. The policy lists ten processing purposes that supposedly rely on the second lawful ground (see Table 1). While most of these appear to be fairly straightforward, one processing purpose in particular merits closer attention: 'personalise the content you receive and provide you with tailored content that will be of interest to you' (7). This is a particularly broad-defined purpose, that appears to challenge the generally strict interpretation of Article 6(1)b as explained above. Especially because content personalisation appears to be primarily aimed at capturing users' attention, but not necessary to access, let alone create content on the platform per se. The EDPB Guidelines specify that:

> personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases. Whether such processing can be regarded as an intrinsic aspect of an online service, will depend on the nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalisation. Where personalisation of content is not objectively necessary for the purpose of the underlying contract, for example where personalised content delivery is intended to increase user engagement with a service but is not an integral part of using the service, data controllers should consider an alternative lawful basis where applicable.[93]

Apart from the fact that one needs to assess whether the *purpose* is necessary for the performance of the contract, it is also important to look if *all* respective personal data processed for that purpose is effectively necessary to achieve that purpose as well (see Section 2.1, 'Purpose Limitation and Data Minimisation'). In other words, even if it is concluded that the processing purposes can legitimately rely on Article 6(1)b, this does not imply that the actual personal data processed is *necessary* to achieve said purpose. *In casu*, it is unclear *what* personal data TikTok exactly uses for personalisation purposes under (7). Indeed, as mentioned before, the Privacy Policy fails to clearly constrain what personal data is used for what purposes. Hence, one can only assume that TikTok entitles itself to use nearly all personal data mentioned in the Privacy Policy for personalisation purposes. This would clearly violate the purpose limitation[94] and data minimisation principles.[95]

Without discarding the above, some personalisation can legitimately be expected by data subjects to be *necessary* for the performance of the contract. This is true, for example, for users with an account, following specific other users and/or hashtags. The second lawful ground can therefore be relied on to the extent that the processing for personalisation purposes is strictly confined to these specific data points, that inherently imply signals from

What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?'
See: European Data Protection Board (n 48) 10.

[93] European Data Protection Board (n 48) 15–16. Emphasis added.

[94] Art.5(1)b GDPR

[95] Art.5(1)c GDPR.

data subjects to finetune their content stream. Currently however, **because TikTok fails to be specific enough in defining the personal data (processing operations) underlying the content-personalisation purposes, they cannot legitimately rely on Article 6(1)b as a lawful ground.**

3.3. Legitimate interests

TikTok's Privacy Policy lists thirteen items under the sixth and last lawful ground (see Table 1).[96] Put very briefly this last lawful ground[97] has three cumulative requirements: (a) *necessary* for the purpose of the (b) *legitimate interests* pursued by the controller or a third party; and (c) *no overriding interests* or fundamental rights and freedoms of the data subject.[98] Moreover, the GDPR emphasises that the last requirement should in particular consider whether the data subject is a child. If children are involved, their interests may override those of the controller more easily, implying a heavier responsibility for controllers using this ground for processing (see below, Section 5).

What can be observed already is that, similarly to the other lawful grounds, it is problematic that TikTok's Privacy Policy is silent about what personal data (or *how* it is processed) exactly feeds into each processing purpose relying on Art.6(1)f. For example, how exactly is personal data processed for the purposes (16) 'promote popular topics, hashtags and campaigns on the Platform' or (22) 'inform our algorithms so we can deliver the most relevant content to you and to prevent crime and misuse of the Platform' and how does this differ from the personalisation purposes for which TikTok relies on the second lawfulness ground for (see above)? The Privacy Policy also mentions Art.6(1)f is relied on for processing personal data involved in verifying the age of its users. Again, it is unclear what exactly this processing entails beyond simply asking to enter a birthday upon registration. As a result, **TikTok renders it is impossible to assess whether it respects the first and last requirement of Article 6(1)f: i.e. necessity and whether the interests, rights or freedoms of data subject override. Simply stating that it has conducted a balancing test, without further details and clear specification on how the different balances can (not) be challenged, should be considered insufficient.**

4. Data protection by design and security

The GDPR installs robust duties on controllers' shoulders to ensure adequate levels of security and data protection. This notably flows from the integrity, confidentiality[99] and accountability

[96] It is not entirely clear to what extent these items concern *interests* rather than *purposes* per se. Both need to be provided in accordance with transparency requirements.
[97] Article 6(1)f GDPR.
[98] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (n 50); AG Opinion in: *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* (n 88) para 62.
[99] Article 5(1)f GDPR.

principles,[100] as well as the provisions on controller responsibility,[101] data protection by design and by default[102] and security of processing.[103] How exactly these obligations are given shape in practice will have to be informed by the nature, scope, context and purpose of processing as well as the risks it poses.[104]

TikTok claims to take 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk that may be posed to you and other users.' Yet, at the same time, TikTok disclaims any responsibility, declaring that they cannot guarantee the security of users' information and 'any transmission is at your own risk'.[105] While there is no strict obligation to communicate to data subjects the exact security measures taken, controllers cannot exonerate themselves from the integrity and confidentiality principles[106] or security requirements[107].[108] Moreover, they need to be able to demonstrate compliance with these provisions at any time.[109] A number of important security issues that were brought to light recently,[110] raise serious questions as to TikTok's compliance with its GDPR security obligations.

The data protection by design and by default requirements[111] are horizontal provisions that, just like controller responsibility[112] and the fairness principle,[113] inform the implementation of all rights and obligations in the GDPR. It is hard to assess compliance with these requirements, purely from TikTok's Privacy Policy. That said, the frequent substantial changes of TikTok's Privacy Policy over the last few years (see above, Section 0), indicate that data protection was not properly considered at the design stages of the service at all. Other examples suggesting the data protection by design and by default requirements are not taken to heart include the

[100] Article 5(2) GDPR.
[101] Article 24 GDPR.
[102] Article 25 GDPR.
[103] Article 32 GDPR.
[104] Article 24(1). Similarly, see *Google Spain* (n 42) [83].
[105] Such security risks are not purely hypothetical, as recently illustrated by a security flaw that enabled hackers to e.g. upload videos and make private videos public. See: Geary, Jasmine. "Serious TikTok Security Flaw Uncovered – and It's Already Been Patched." *TechRadar*, January 9, 2020. https://www.techradar.com/uk/news/serious-tiktok-security-flaw-uncovered-and-its-already-been-patched.
[106] Article 5(1)f GDPR, requiring that personal data 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.'
[107] Article 32 GDPR.
[108] See also: European Data Protection Board, 'Data Protection by Design and by Default (v2.0)' (Guidelines, 20 October 2020) 27–28.
[109] Article 5(2) and 30(1)g GDPR.
[110] Ivan Mehta, '235M Instagram, TikTok, and YouTube Profiles Exposed in Database Breach' (*The Next Web*, 20 August 2020) <https://thenextweb.com/security/2020/08/20/235m-instagram-tiktok-and-youtube-profiles-exposed-in-database-breach/> accessed 22 January 2021; Zak Doffman, 'Beware If You Use TikTok On Your IPhone: Here's Why You Should Now Worry—New Security Report' (*Forbes*, no date) <https://www.forbes.com/sites/zakdoffman/2020/03/12/simple-apple-security-hack-if-you-have-tiktok-on-your-iphone-look-away-now/> accessed 14 December 2020; 'TikTok Spying on Its Users and Massive Security Issues?' (*Cybr*, 7 May 2020) <https://cybr.com/cybersecurity/tiktok-spying-on-its-users-and-massive-security-issues/> accessed 25 November 2020.
[111] Article 25 GDPR. See notably also : European Data Protection Board (n 111).
[112] Article 24 GDPR.
[113] Article 5(1)a GDPR.

fact that the Privacy Policy does not foresee a special regime for the processing of 'special categories of personal data'[114] or the processing of personal data of under eighteen-year-olds (see below).

5. (Lack of) Special protections for children

The GDPR requires special protection for children when it comes to the processing of their personal data, as they are less aware of the risks and the potential consequences of such processing on their rights (Recital 38 GDPR).[115] Children merit such specific protection *particularly* in situations where their personal data is used for (1) marketing purposes, (2) for the creation of profiles and (3) for the collection of their data when using services offered directly to a child (Recital 38 GDPR). Important to underline is that a 'child' under the GDPR is anyone under 18 years, in line with the UN Convention on the Rights of the Child.[116] Thus, without clear guarantees in TikTok's Privacy Policy that children – anyone under 18 – are offered such special protection when their personal data are processed, TikTok is in violation of this GDPR requirement as well as several other GDPR provisions.

In particular, the following elements are missing from the Privacy Policy and/or TikTok's design of the service:

Missing elements	Violation of GDPR	Age category affected
Special protection measures for children	in violation of Recital 38 GDPR	all TikTok users under 18
Special protection for children in the context of profiling	in violation of Recitals 38 and 71 GDPR	all TikTok users under 18
Child-centred approach to the design of the TikTok service in the EU	in violation of Article 25 GDPR read together with Recital 38 GDPR	all TikTok users under 18
Special protection measures upon registration to enforce the cut-off age of 13[117]	in violation of Article 8 GDPR	all TikTok users under 13

[114] Article 6 GDPR.

[115] Moreover, Recital 75 GDPR recognises that the processing of children's personal data may result in risks to the rights and freedoms of natural persons.

[116] See for instance the Article 29 Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), where the Article 29 Working Party refers to article 1 of the UNCRC *"According to the criteria in most relevant international instruments, a child is someone under the age of 18, unless he or she has acquired legal adulthood before that age"*. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf.

[117] This analysis was conducted prior to the announcement of the Italian Data Protection Authority on 22 January 2021 that it would impose an immediate limitation on TikTok's processing of the data of users whose age could not be established with certainty. According to the Italian DPA: *"TikTok responded it would implement measures to ban access to users aged below 13 years and will consider deploying AI-based systems for age verification purposes. An information campaign will also be launched by the company to raise parents' and children's awareness."* It is currently unclear whether TikTok will implement these measures across the EU or only in Italy. See https://edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_en; and https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424#english_version.

Mechanism for verifiable parental consent that respects the various age thresholds as selected by the different EU Member States	in violation of Article 8 GDPR	all TikTok users below the age threshold of consent in their respective EU Member State

Table 2 - Overview of issues regarding the protection of children in TikTok's Privacy Policy

These issues are discussed in more detail below, categorised on the basis of the different age groups affected: (a) all TikTok users under 18; (b) TikTok users below the age of 13 ("barred users") and (c) TikTok users aged 13-17.

5.1. All TikTok users below the age of 18

What is perhaps most striking about TikTok's Privacy Policy is that it does not appear to distinguish children from adult users at all.[118] Therefore, the Privacy Policy allows TikTok to carry out the same practices concerning profiling and the processing of personal data for targeted advertising purposes on adult- and child-users of the service. This is **contrary to the GDPR's requirement that special protection needs to be awarded to children** when their personal data are processed, and particularly in the context of profiling and marketing (Recital 38 GDPR).

Furthermore, the processing of personal data *'in order to create or use personal profiles'* may give rise to risks to the rights and freedoms of natural persons.[119] The preamble of the GDPR provides a twofold protection for children in relation to **profiling**. First, circumstances in which personal data of children are processed in order to create personal or user profiles are explicitly acknowledged as requiring additional protection.[120] Second, according to recital 71, a decision that may include a measure evaluating personal aspects relating to a data subject that is based solely on automated processing should not concern children.[121] However, this is only prohibited as far as a decision produces legal effects for, or similarly significantly affects the child. Targeted advertising may, depending on the particular characteristics of the case, have a 'similarly significant' effect on individuals. Especially in relation to children, the Article 29 Working Party recognises that they *"can be particularly susceptible in the online environment and more easily influenced by behavioural advertising"* and, therefore, *"organisations should, in general, refrain from profiling them for marketing purposes."*[122] Aside from targeted advertising, TikTok's recommender system has also been shown to differentiate based on, for example, 'abnormal body shape' and 'ugly facial looks', which can be considered to significantly impact the respective data subjects whose content is labelled as such.[123] Considering that TikTok's Privacy Policy allows it to profile and target users under

[118] Subsection 9 mentions children: *"TikTok is not directed at children under the age of 13..."* – see Excerpt 5 below.
[119] Recital 75 GDPR underlines that the processing of personal data may result in a risk to the rights and freedoms of natural persons, in particular *"[...] 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"*.
[120] Recital 38 GDPR.
[121] Recital 71, first paragraph, final sentence GDPR.
[122] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2017) 26.
[123] Köver (n 38); Biddle and Ribeiro (n 38).

18 years with personalised advertising, and treats them no different than it treats adult-users, this does not satisfy Recital 71 read in conjunction with the requirement of special protection.

In addition, Article 25 GDPR requires that controllers should implement appropriate technical and organisational measures to integrate necessary safeguards and protect the rights of data subjects and to ensure that, by default, only personal data that are necessary for each specific purpose of the processing are processed (see above, Section 4). Moreover, data controllers should build in a specific level of protection for all children under 18 accessing their services into the technology and the offer of services, and use different default settings. Such a child-centred approach to the design of online services has also been recommended by the Council of Europe.[124] In the US, TikTok already offers a specific service for under 13s (after reaching a settlement with the Federal Trade Commission)[125] but, at the time of writing, this service is not available in the EU. Thus, **TikTok does not satisfy Article 25 GDPR read in conjunction with the requirement of special protection for children.**

There is currently no information available about whether or not TikTok has conducted a Data Protection Impact Assessment (DPIA). Article 35 GDPR requires controllers to assess the impact of processing operations that are likely to result in a high risk to the rights and freedoms of data subjects. Recital 91 states that a DPIA must be carried out when personal data are processed for taking decisions regarding specific natural persons based on profiling.[126] When children are involved, such a DPIA should adopt a children's rights perspective that takes into account the full range of children's rights at stake as well as the best interests of the child.[127] If TikTok did conduct a DPIA, it would be useful for the company to communicate (a summary of) the findings, or at least notify users of the existence of a DPIA, as this could contribute to user confidence and data protection by design. Data protection authorities could also request more information from TikTok about their DPIA.

5.2. TikTok users aged 13-17

Article 8 GDPR allows Member States to lower the age threshold for consent to a minimum of 13 years. As a result, different age thresholds apply throughout the EU and TikTok has to adapt its Privacy Policy and settings in accordance with the various national implementations of Article 8.[128] In other words, in those EU Member States where the age threshold for consent is above TikTok's cut-off age of 13 (e.g. 16 in the Netherlands) TikTok should also

[124] Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers (2018), Guidelines to respect, protect and fulfil the rights of the child in the digital environment, https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html.
[125] For more information see https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its.
[126] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
[127] S. van der Hof and E. Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR' (2018) 23 Communications Law 33.
[128] For an up-to-date overview see https://www.betterinternetforkids.eu/nl/practice/awareness/article?id=3017751.

obtain verifiable parental consent for child-users between 13-15. **TikTok's Privacy Policy for residents of the EEA currently does not satisfy this requirement.**

It should be acknowledged that there have been **significant changes to improve** the protection of child–users aged 13-17. First, a 'Family Pairing' functionality has been introduced, so as to *'customise your teen's TikTok settings for a safer experience*' (i.e. set time limit, limit content that isn't suitable, limit who can send messages, public/private account).[129] Although it is a laudable initiative to encourage more parental involvement in children's online activities, it also raises a number of concerns. Not all parents are necessarily better equipped than their children when making decisions about processing of personal data. Also, in certain situations it is conceivable that parents are not online or simply not present. If TikTok were to rely on this feature as a means to shift the burden of child protection onto the shoulders of parents, this would of course be in clear breach of its duties under the GDPR.

Second, TikTok now offers a summary of its Privacy Policy for users between 13 and 18 years. This is in line with the requirement for data controllers to provide information in a child-friendly manner (i.e. *'such a clear and plain language that the child can easily understand*').[130] However, this summary is only available in the TikTok App and not via the web-version, which means that TikTok's information obligation will not be fulfilled in relation to children who only access the web-version. Children are also not prompted to read the summary and have to search for it.

Third, in an update on 13 January 2021, TikTok enhanced its default privacy settings.[131] More specifically, the default for all registered accounts aged 13-15 was changed from public[132] to private.[133] However, it can be questioned why this measure was not extended to all children under 18 years.

From these updates it is clear that TikTok is investing in its protection of this age group of users, though mostly in relation to the platform's 'social privacy settings' and still treating this age group as adults when it comes to the use of their personal data for marketing (and other business-related) purposes.

[129] For more information see https://newsroom.tiktok.com/en-us/supporting-youth-and-families-on-tiktok.
[130] Recital 58 and Article 12(1).
[131] Eric Hahn, Strengthening privacy and safety for youth on TikTok, https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth.
[132] Previously, the default setting for video sharing and the account itself is 'public' and an App user can direct message any other user - which is not 'child-friendly' by default.
[133] TikTok explains that '[w]ith a private TikTok account, only someone who the user approves as a follower can view their videos. We want our younger users to be able to make informed choices about what and with whom they choose to share, which includes whether they want to open their account to public views. By engaging them early in their privacy journey, we can enable them to make more deliberate decisions about their online privacy.' Eric Hahn, Strengthening privacy and safety for youth on TikTok, https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth.

5.3. Children below the age of 13 using TikTok ("barred users")[134]

For the provision of targeted advertising, TikTok's Privacy Policy states that it relies on the data subject's consent as the lawful ground for processing. As mentioned before, Article 8 GDPR contains specific requirements regarding consent for the processing of personal data of children. The general rule provides for a parental consent requirement for all children under 16 years old in situations where information society services are offered directly to them, and consent is the lawful ground on the basis of which the data is processed. However, Member States may choose to deviate and decide to lower this age threshold to 15, 14, or 13 years. TikTok is an 'information society service', which is defined as *'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'*[135] Such services do not necessarily require payment by the users themselves, and services financed by advertising would also fall under this definition (i.e. the alleged 'free' services such as social media, search engines, news portals, etc.). TikTok's Privacy Policy claims that it is not directed at children under the age of 13 (Excerpt 6).

> TikTok is not directed at children under the age of 13. If you believe that we have personal data about or collected from a child under the relevant age, contact us at: https://www.tiktok.com/legal/report/privacy.

Excerpt 6 - Information relating to children

However, the Article 29 Working Party has clarified that 'if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be "offered directly to a child" and Article 8 will not apply' (emphasis added).[136] Research has shown that a significant percentage of TikTok users are children under the age of 13,[137, 138] and this has also been widely addressed in press coverage.[139] In addition, a big portion of the content of the site is clearly aimed at children. For instance, the App's online music library includes millions of song tracks, including songs from popular children's movies and songs popular amongst younger children.[140] Moreover TikTok does not employ an age verification mechanism but merely

[134] This analysis was conducted prior to the announcement of the Italian Data Protection Authority on 22 January 2021 that it would impose an immediate limitation on TikTok's processing of the data of users whose age could not be established with certainty. It is currently unclear whether TikTok will implement additional protection measures upon registration across the EU or only in Italy (see also footnote 117).

[135] Article 4 (25) GDPR refers to 'information society service' as "a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council".

[136] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) 25.

[137] See BEUC Report, (2021), *TikTok without Filters*, Section 1.

[138] For instance in Flanders, a 2020 study has shown that 44% of Flemish 6-12 year-olds uses TikTok: available at https://drive.google.com/file/d/12D3iqTTIaXpLy5EIeIqs-u19AKsX8mtr/view; similarly in the Netherlands, the App is actually most popular among children under 13: http://www.multiscope.nl/persberichten/1-miljoen-tiktok-gebruikers-in-nederland.html.

[139] Some examples of newspaper articles in Flanders, https://pub.be/nl/apestaartjaren-jongeren-grijpen-steeds-vroeger-naar-digitale-media/; https://www.vrt.be/vrtnws/nl/2020/05/27/_kinderen-hebben-steeds-jonger-een-smartphone-ze-hebben-dus-vr/.

[140] This was also used as evidence by the FTC complaint against TikTok (formerly known as musical.ly) https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf.

relies on self-reported age users during registration, which is easily circumventable. No other apparent measures to mitigate the risk of children under 13 years accessing the App are relied upon. In short, TikTok claiming the cut-off age to the service is 13 years, is undermined by the content of the App and the lack of age verification or other mitigation measures. Moreover, independent research has established that significant portions of under 13-year olds are in fact using the platform.

From the above, it follows that **TikTok's Privacy Policy and its lack of special protection measures upon registration allows the processing of personal data of children under 13 (among others, for targeted advertising purposes), without obtaining nor verifying parental consent, which is in breach of article 8 GDPR.**

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme.

cc BY NC