




# Children and Data Protection

How the term ‘specific protection’ for children under the GDPR should be implemented by social media platforms

#### Interactief

Om door de pagina's te bladeren klik je op de iconen   om respectievelijk naar de vorige of volgende pagina te gaan. Om terug te gaan naar de inhoudsopgave klik je op  icoon. Bij de inhoudsopgave zijn de hoofdstukken aanklikbaar.



## Table of contents

Executive summary	5
1 Introduction	7
2 Legal Framework	9
3 Problems with 'specific protection' in practice	12
4 Explanation of the norm 'specific protection'	14
1 No Personalised Advertising	14
2 No Automated Profiling	15
3 Child-specific Privacy Policies	16
Justification	22

# Executive summary

According to the GDPR, platforms must offer ‘specific protection’ to children with regard to the processing of their personal data (recital 38 GDPR). The GDPR provides little guidance on the interpretation of this term. It contains rules specifically regarding children in article 8 GDPR on parental consent and in article 12 GDPR on the obligation to provide clear and comprehensible information regarding the processing of personal data. Besides these measures, it is not clear what other ‘specific protection’ a child is entitled to.

We notice in practice, that social media platforms only provide specific protection through the implementation of articles 8 and 12 GDPR. More importantly, we see that the policies employed by social media platforms, based on these articles, do not fulfil their purpose in practice.

First: requiring parental consent only works when a child is being honest. But children can lie easily online, and more effective methods for age verification are privacy-intrusive. This is why we believe parental consent does not contribute to an effective solution on how to provide specific protection to children. Second: the privacy policies of several social media platforms we examined were long and difficult for a child to understand.

The platforms we have examined provide no additional protection to children beyond this. In fact, profiling children and showing personalised advertising to them – problematic already for adults and even more so for children – is part of every platform’s business model. We believe this is not compatible with the obligation to provide ‘specific protection’ to children.

It is therefore necessary to clarify how organisations can provide the ‘specific protection’ a child is entitled to. We conclude that social media platforms should provide specific protection for children on three different aspects: their privacy policies, profiling, and personalised advertising. We encourage the Dutch DPA and EDPB to develop these standards for the protection of children’s privacy online into guidelines.

## **No personalised advertising for children**

Personal data of children under 16 years should not be processed for personalised advertising. Although personalised advertising is not explicitly prohibited under the GDPR, we believe that targeting children for personalised advertising will always exceed the boundaries of lawful and fair processing. Companies should not be able to ask platforms to specifically target children. Where a platform suspects, or should reasonably suspect that an advertisement is intended towards children, it should err on the side of caution and not accept the ad for personalised advertising purposes. Platforms are allowed to pursue their own commercial interests, but these should never be incompatible with the best interests of a child. At this young age, the prevention of exploitation of the child always has to come first. To be clear: children may still be presented with contextual or untargeted advertising, but this should be

clear to them. This could be achieved with a pop-up, an icon, or a short message next to the advertisement.

### No profiling of children for personalised content

Profiling children for personalised content may not be based on algorithms. Content which children see should only be based on preferences they indicate themselves. As children are still developing, timelines and home pages it should further be considered to not only show personalised content, but also include content from other topics, so as to promote a more diverse range of information and prevent 'filter bubbles'. Furthermore, children's personal data should be reviewed for retention at least yearly. Data which are no longer relevant or necessary to process should be removed as in line with the principle of data minimisation (article 5(1)(c) GDPR).

This data on interests and preferences should further not be sold to third parties, as this generally will not be compatible with the purpose for which the data were originally gathered, given the vulnerability of children. Platforms should also refrain from linking data from children from different platforms or datasets, as this may also infringe the purpose limitation and data minimisation principles.

### Inform children better

As platforms process data from children differently than that from adults, they should create separate information on processing for children. This information should be clear and comprehensible. Audio-visual aids should be used to help understand the processing taking place. The information should be in the common spoken language of the country where the service is used: English is not enough. Besides, long texts and difficult language will deter children from reading the policies. The separate privacy policy for children must be in a clear language and be simple and concise. Visual support is encouraged.

Although clearer privacy policies should answer most questions a child may have, social media platforms should in addition create a help desk for more in-depth questions concerning their account and their personal data. We believe this is a basic consumer right which platforms should not be exempted from.

# 1 Introduction

Processing of personal data is particularly important for social media platforms which base their business model on personalised advertising to their users. The General Data Protection Regulation (hereafter: GDPR) provides some protection against this processing. For example, in many cases, the data controller must obtain consent of the data subjects before personal data may be processed.

Children are also active on social media, in fact, they are one of the largest consumer groups.<sup>1</sup> But they are less aware of the risks and consequences involved in the processing of personal data and are more susceptible to be influenced. Unfortunately, this makes them also very interesting to (behavioural) advertisers. A big tech company that develops student learning applications, even stated that their goal is to actively change children's behaviour, rewarding good and punishing bad behaviour.<sup>2</sup> Because children are more susceptible to these influences, they should be given specific protection according to the GDPR. For example, parents of children under the age of 16 must give their consent before their children's personal data can be processed under the consent ground. In practice, this creates two problems.

First of all, children need privacy, also towards their parents. Children do not want their parents to always know what they are doing, and they may see parental consent more as parental control.<sup>3</sup> That is why children will not always want to ask for their parents' permission when they go on social media. This creates a 'vacuum' for children who go online themselves, often also have their own smartphone, create a profile on social media, but still need extra protection.

Secondly, social media platforms find it difficult to check whether children under the age of 16 have received permission from their parents, and it is not directly to their advantage to develop a robust age check, because this creates an extra duty of care for them. Submitting a fake, older age is very easy for a child and often the only way to avoid parental control. Consequently, these children may not get the mandatory specific protection the GDPR requires.

Besides the problem of consent, the GDPR is unclear on how to provide the 'specific protection' a child is entitled to. Leaving this consideration up to companies with interests opposed to that of a child, makes the current protection rather weak. More

<sup>1</sup> Unicef, Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World. [https://www.unicef.org/csr/files/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_PRIVACY.pdf](https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf), p. 11

<sup>2</sup> Zuboff, Shoshana, 'The Secrets of Surveillance Capitalism', Frankfurter Allgemeine, 5 March 2016, available at [www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616-p2.html](http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616-p2.html)

<sup>3</sup> S. van der Hof, Children and data protection from the perspective of children's rights - Some difficult dilemmas under the General Data Protection Regulation Kluwer: 2018, p. 14

clarity on how to implement this provision would strengthen this protection. Accordingly, this report will set a number of minimum standards which social media platforms should abide by in order to provide an adequate 'specific protection' to children.

In this report, we focus on children between 8 and 16 years old. From 8 years of age, children go online themselves, and often have their own smartphone. Under Dutch law, children from the age of 16 no longer need to be given consent by their parents.

The aim of the report is to create a standard for the provision 'specific protection'. This specific protection is aimed to protect children from the social media platforms itself. Although we believe that children should be protected from other users, such as predators, we do not go into this matter since this lies outside the scope of this report.

In the first chapter, we will set out the legal framework around the processing of children's data. Then, we will explain why it is a problem that the term 'specific protection' lacks further explanation. We end this report with a chapter on how this term should be explained by creating several standards that should be applied when processing children's personal data.

## 2 Legal Framework

According to the GDPR, the processing of personal data is only lawful if one of the conditions of Article 6 is met:

- a. Consent has been given by the data subject;
- b. The processing of data is necessary in order to execute an agreement;
- c. The processing of data is necessary to comply with a legal obligation;
- d. The processing of data is necessary to protect vital interests;
- e. The processing of data is necessary for the performance of a task carried out in the public interest or in the exercise of public authority; or
- f. The processing of data is necessary in order to protect the legitimate interests of the data controller.

While personal data need to be processed for the operation of social media platforms, personal data are also in large part collected and used for personalised advertising. This is almost always based on consent, since profiling – especially with children – is a processing operation that, due to the relatively high risks of privacy infringement, in many cases will not be able to be considered as a legitimate interest as referred to in article 6 paragraph 1(f) GDPR.<sup>4</sup> Profiling is defined as the (automated) processing of personal data to evaluate, analyse or predict aspects relating to a natural person, such as their behaviour, preferences and interests.<sup>5</sup> The data controller must also be able to demonstrate that consent has actually been granted to meet its accountability obligations (Art. 5(2) and Art. 7(1) GDPR).

According to the GDPR, children are entitled to specific protection with regard to their personal data, since they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Children are still developing and learning. They are easily influenced, cannot fully understand the consequences of their actions and are gullible. They may thus not always notice that an advertisement is shown or that certain content is specifically targeted to them. For example, a study of children of 8 to 15 years old showed that only a minority of children can identify sponsored links in search engine results, despite their being distinguished by a green box with the word 'Ad' in it.<sup>6</sup>

This "specific protection" that the GDPR imposes is not well explained in the GDPR. It is stated in the preamble (recital 38 GDPR) that this specific protection should apply in particular to the use of children's personal data for marketing purposes, the

<sup>4</sup> In order to be able to invoke this ground, the controller must always determine whether its own interest overrides the user's right to privacy. The Dutch DPA takes the view that a purely economic interest – a higher profit margin through more effective advertising, for example – can never be considered justified. See Autoriteit Persoonsgegevens 'Normuitleg grondslag 'gerechtvaardigd belang'. Although this view is contested in VoetbalTV/AP (ECLI:NL:RBMNE:2020:5111), we still believe that the processing of children's personal data for marketing purposes will be done in most cases on the basis of consent.

<sup>5</sup> Article 4(4) GDPR.

<sup>6</sup> Ofcom, Children and Parents: Media Use and Attitudes Report, 4 February 2020, p. 153

creation of personality or user profiles and the collection of personal data about children when using services provided directly to children. This is partly elaborated in article 8 of the GDPR. This article applies when a service is directly targeted at a child, and states that a child of at least 16 years of age can provide valid consent. For children below this age, consent must be given by a person having parental responsibility over them. This age limit of 16 may be reduced to a minimum of 13 years under national law. The Dutch GDPR Implementation Act (hereafter: UAVG) does not currently make use of this possibility, but many other Member States have a lower age minimum.

According to the European Data Protection Board (hereafter: EDPB), Article 8 GDPR does not apply if a service provider makes it clear to potential users that the services are only offered to persons aged 18 years or older, and this is not undermined by other evidence (such as the content of the website or marketing plans).<sup>7</sup> However, the social media platforms we studied do offer services to children. Among other things, they offer child-friendly content, display personalised advertising especially for children, and children can create their own profiles. That is why we consider article 8 GDPR to be applicable to them. In any case, the UAVG contains an additional rule, where consent from a guardian is still required in cases where article 8 GDPR is not applicable to children.<sup>8</sup> Parental consent is therefore always necessary in the Netherlands where children under 16 years are using the social media platforms we studied.

In addition, information and communication aimed specifically at a child must be written in such a clear and simple language that the child can easily understand it (recital 58 and article 12(1) GDPR). Article 29 Working Party (the predecessor of the EDPB, hereafter: WP29) stated that “controllers should consider what types of measures may be particularly accessible to children (e.g., these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).”<sup>9</sup> Privacy statements for children must use clear language and be simple and concise. This can be done through visual support as proposed by the WP29. The Dutch Supervisory Authority (hereafter: AP) takes the same position.<sup>10</sup>

One of the tasks that the GDPR sets for data protection authorities, is to “promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention.”<sup>11</sup> The ICO, Britain’s data protection authority, has prepared a code of practice containing guidance on standards of age-appropriate design for platforms that are likely to be accessed by children.<sup>12</sup> The Code came into force in September 2020, with a 12-month transition period. It includes standards

7 European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, para. 7.1.2.

8 Article 5 Uitvoeringswet Algemene verordening gegevensbescherming.

9 Article 29 Working Party, Guidelines on transparency under regulation 2016/679, para 18

10 <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#waar-moet-u-op-letten-als-u-gegevens-van-kinderen-verwerkt-op-basis-van-toestemming-7527>

11 Article 57 (1)(b) GDPR.

12 Section 123 (1) UK Data Protection Act 2018.

such as prioritising the best interests of the child, having ‘high privacy’ settings be turned on by default, and only allowing profiling if child-appropriate protective measures have been taken. The AP and EDPB would do well adopting a similar guideline.

Article 40(2)(g) GDPR specifically calls for the drawing up of codes of conduct regarding the protection of children. The FEDMA Code of conduct is such an example, setting rules on how marketing to children should be handled. Section 6.2 of this Code states that marketers should not exploit children’s vulnerabilities, while section 6.8.5 states that children should not be obligated to consent to personal data collection.<sup>13</sup> These codes of conduct are intended to contribute to the proper application of the GDPR, however, and the FEDMA Code was adopted in September 2000. It seems that it is high time for an update.

Children are a more vulnerable group of society. They can be particularly prone to the influence of behavioural advertising in the online environment, as normal content and advertising blend together seamlessly. Some companies use profiling to target players who, according to an algorithm, are more likely to spend money on microtransactions in the game. When it comes to children, age and maturity may affect whether they understand the motives of behavioural targeting.<sup>14</sup> The WP29 repeatedly argued that behavioural advertising is outside of the scope of a child’s understanding, and thus data controllers should not process children’s data for this purpose, as it would exceed the boundaries of lawful and fair processing.<sup>15</sup>

In summary, online service providers addressing children directly should take certain additional measures to ensure the required additional protection of children. Platforms should seek parental consent for children under the age of 16 and should communicate clearly with the child about the data processing taking place. In addition, as a service provider has a general accountability responsibility, it must be able to demonstrate that it complies with the additional safeguards of the GDPR. Besides these measures, it is not clear what other ‘specific protection’ a child is entitled to, but using children’s personal data for behavioural targeting does not seem to be compatible. As the GDPR leaves room for improvement, the next chapters will discuss possible avenues to provide children with a balanced specific protection.

13 Available at: <http://www.oecd.org/sti/ieconomy/2091875.pdf>

14 An EU [study on the impact of marketing through social media, online games and mobile applications on children’s behaviour](#) found that personalised advertising has a clear impact on children’s behaviour. This study concerns children between 6 and 12 years old.

15 WP29 Opinion 02/2013 on apps on smart devices (WP202) para. 3.10; WP29 Opinion 2/2010 on online behavioural advertising, para 4.1.4; WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, para V.

### 3 Problems with ‘specific protection’ in practice

As discussed above, although the GDPR sets a few rules on how children’s personal data may be processed, there is no clear explanation of the norm ‘specific protection’. This results into a situation where only the clear rules laid down in article 8 and 12 GDPR are being followed. In preparation of this report, we investigated the privacy policies of the current biggest social media platforms among children.

We found two things. Firstly, these platforms do not take other protection measures for children’s personal data besides asking for parental consent and giving clear and comprehensible information about the processing of personal data (and even this information was often not very clear). Our detailed findings can be found in Annex I.

Second, even this limited measure of parental control and related age verification does not work in practice. Parental consent is currently only properly regulated when the child is honest. In many cases, however, a child will not want to ask his or her parents for permission.<sup>16</sup> It is very easy to fill in an older age and this is not verified. According to the EDPB, collecting data from children who themselves give consent is unlawful. This means that a self-declared age is not sufficient to verify an age. We have at the same time found that the platforms in our study take no reasonable efforts to verify whether a parent has given consent. Each platform that we examined checks the age by letting the child fill in its age. Accordingly, each of these platforms are in breach of the GDPR if children are on their platform without valid consent.<sup>17</sup>

Conversely, platforms must also comply with the principles of data minimisation, purpose limitation, accuracy, and relevance (article 5 GDPR). The retrieval of passport data or a DigiD would strengthen age verification, but could be contrary to the principle of data minimisation. The ICO, also warns social media platforms that they should not use nudge techniques, which could lead to children lying about their age.<sup>18</sup> There is as of now no clear answer how age verification should be carried out on a platform whereby it is not possible to lie about age and all the principles of article 5 GDPR are guaranteed.<sup>19</sup> For this reason, we believe parental consent and age verification by monitoring behaviour do not contribute to an effective solution on how to provide specific protection to children.

<sup>16</sup> S. van der Hof, Children and data protection from the perspective of children’s rights - Some difficult dilemmas under the General Data Protection Regulation Kluwer: 2018, p. 14

<sup>17</sup> European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, para. 7.1.3

<sup>18</sup> See ICO, “Age appropriate design: a code of practice for online services”. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/13-nudge-techniques/>

<sup>19</sup> Livingstone, Sonia (2018) Children: a special case for privacy? *Intermedia*, 46 (2). pp. 18-23. ISSN 0309-118X

Following the above, two problems occur. First, social media platforms do not provide specific protection concerning the processing of children’s personal data besides the rules set out regarding parental consent and clear and comprehensible information. Second, we see that the rules laid down by social media platforms do not fulfil their purpose in practice. Children’s personal data are part of social media platforms’ business models. As explained above, children can be easily influenced, do not oversee certain consequences, are gullible and therefore can be easily exploited. Social media platforms should take their responsibility and protect children on their platform, not only for other users, but also for the platform itself.

Considering the above two problems, we believe that an explanation of the norm ‘specific protection’ will clarify what social media platforms should do when processing children’s personal data and it will strengthen this provision. The next chapter will give a framework of standards which social media platforms should implement.

## 4 Explanation of the norm ‘specific protection’

Article 24 of the EU Charter of Fundamental Rights states:

**“In all actions relating to children, whether taken by public authorities or private institutions, the child’s best interests must be a primary consideration.”**

The specific protection provided by the GDPR should therefore be in line with the child’s best interests. While this does not mean that social media platforms can never pursue their own commercial or other interests, they need to account for the best interests of the child as a primary consideration where any conflict arises.<sup>20</sup> The EPDB states that consent is only valid if denying it has no negative consequences.<sup>21</sup> This consideration should also apply here, in the sense that submitting an age under 16 years should not have any negative effects on the overall experience of children on social media platforms. After all, this would not be in the best interest of children, concerning their right to freedom of expression, access to information and development of digital literacy.<sup>22</sup>

Social media platforms should provide specific protection for children on three different aspects: personalised advertising, profiling, and their privacy policies.

### 1 No Personalised Advertising

**Personal data of children under 16 years should not be processed for personalised advertising.**

Although personalised advertising is not explicitly prohibited under the GDPR, we believe that targeting children for personalised advertising will always exceed the boundaries of lawful and fair processing.<sup>23</sup> Platforms are allowed to pursue their own commercial interests, but these should never be incompatible with the best interests of a child. At this young age, the prevention of exploitation of the child will always come first.<sup>24</sup> This is also in line with the position of the EDPB, which stated in

20 See also: ICO. “Age appropriate design: a code of practice for online services”. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/>

21 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, point 13.

22 Unicef, Privacy, protection of personal information and reputation rights. Discussion paper series: Children’s Rights and Business in a Digital World. [https://www.unicef.org/csr/files/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_PRIVACY.pdf](https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf), p. 9

23 These are two of the main principles of the GDPR, see article 5 (1)(a) GDPR.

24 See also: ICO. “Age appropriate design: a code of practice for online services”. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/>

several recommendations that children’s personal data should not be processed at all for personalised advertising.<sup>25</sup> This report does not recommend the implementation of stronger parental consent mechanisms or active age verification. Instead, platforms should act according to the contents of advertisements. Companies should not be able to ask platforms to specifically target children. Where a platform suspects, or should reasonably suspect that an advertisement is intended towards children, it should err on the side of caution and not accept the ad for personalised advertising purposes.

Children may still be presented with contextual or untargeted advertising, but this should be clear to them. Studies have shown that launching a campaign on the basis of contextual targeting has a greater influence than launching a non-contextual campaign.<sup>26</sup> Using this form of advertising can be more effective than personalised advertising, if used in the right context. A business model with only contextual or untargeted advertising to children finds a balance between the best interests of the child and the commercial interests of the social media platform.

While contextual and untargeted advertising are more privacy-friendly than personalised advertising, they are not without risk. Awareness and literacy should be promoted under children. This could be achieved with a pop-up, an icon, or a short message next to the advertisement. This pop-up can also refer the child to its parents, for example: “If you are not sure what the above message means, make sure you consult your parents or an adult.”<sup>27</sup>

### 2 No Automated Profiling

**Profiling children for personalised content should not be based on algorithms. Content which children see should only be based on what they indicate themselves. Children’s personal data should never be sold.**

Profiling is defined as the (automated) processing of personal data to evaluate, analyse or predict aspects relating to a natural person, such as their behaviour, preferences and interests.<sup>28</sup> Algorithm-based profiling often leads to ‘filter bubbles’.<sup>29</sup> Children are still developing and should be able to obtain information from different perspectives, without algorithmic reinforcement. Content can still be personalised, but should be done by the user, for instance with prompts which ask

25 See for example WP29 Opinion 02/2013 on apps on smart devices (WP202) para. 3.10; WP29 Opinion 2/2010 on online behavioural advertising, para 4.1.4; Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, para V.

26 Ster, ‘Een toekomst zonder advertentiecookies?’, p. 19. Available at <https://www.ster.nl/media/quakpy4e/ster-eeen-toekomst-zonder-advertentiecookies.pdf>

27 This is also encouraged by ICO. “Age appropriate design: a code of practice for online services”. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/4-transparency/>

28 Article 4(4) GDPR.

29 Quattrociocchi, W., Scala, A., Sunstein, C.R.: Echo chambers on Facebook, SSRN2795110 (2016), p. 14



the user to choose their interests. As children are still developing, timelines and home pages should not only show personalised content, but it should be considered to also include random child-friendly content from other topics, so as to promote a more diverse range of information and prevent ‘filter bubbles’.

Children should be encouraged to exercise control on to which degree their content is personalised, including an option to remove all personalisation (for instance, the option to sort timelines in chronological order). Some services may be specifically centred around personalised content, but these form an exception to the rule.<sup>30</sup> Also without action of the child, the retention of their personal data should be reviewed, at least yearly. Data that are not necessary to process should be removed as in line with the principle of data minimisation (article 5(1)(c) GDPR).

Providing personalised content based on the interests and preferences that children choose themselves, is a different purpose than providing advertisements based on these preferences, and strict purpose limitation should be applied here. Children’s personal data should not be sold to third parties, as this generally will not be compatible with the purpose for which the data were originally gathered. Platforms should also refrain from linking data from different platforms or datasets, as this may also infringe the purpose limitation and data minimisation principles.

### 3 Child-specific Privacy Policies

**As platforms process data from children differently than that from adults, they should create separate information for children. Policies should be short, in clear language, supported by audio-visual media and they should be in the common spoken language of the country where the service is used.**

Children need to understand the data processing taking place. This means using audio-visual aids. In addition, the privacy policy should always be in the common spoken language of the country where the service is used. A child in the Netherlands will in most cases not be able to truly understand the privacy policy if it is only written in English. Besides, long texts and hard language will deter children from reading the policies. The separate privacy policy for children must be in a clear language and be simple and concise. Visual support is essential.

Children should also be involved in the process of creating privacy policies. WP29 proposed that:

***“If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/policies etc., they can test these, for example, through mechanisms such as user panels [...]”***<sup>31</sup>

30 ICO. “Age appropriate design: a code of practice for online services”. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/12-profiling/>

31 Article 29 Working Party, Guidelines on transparency under regulation 2016/679, para 9

These user panels should be set up with child participants. Children are in a better position to judge whether privacy policies are understandable to their peers. In this way, children are able to express their opinion, provide advice and recommendations. Their views must receive due weight.<sup>32</sup>

### Platforms should create a help desk for questions concerning their account and their personal data

Although clearer privacy policies should answer most questions a child may have, social media platforms should create a help desk for more in-depth questions concerning their account and their personal data. Currently, there is no easy way for children to reach social media platforms. Especially children who might want to delete their account or do not know how to change their privacy settings should get the help they need. Help desks are regular in all sorts of businesses. While social media platforms are economies of scale, they should not be exempt from providing such a basic consumer right.

### Concluding remarks

This report focuses on the processing of children’s personal data. The explained norm ‘specific protection’ is based on additional rules for children specifically. We made a selection of three topics where the current situation does not provide a specific protection to children, and where the implementation of our norms could realistically provide a more sufficient protection. However, our norms do not cover all areas where platforms do not yet provide sufficient protection, and other norms that could benefit all data subjects are naturally also applicable to children. We therefore conclude with some additional remarks, which social media platforms could implement as well, in order to comply with the GDPR. We believe that additional research in these areas could prove beneficial.

First: we have explained in this report why we believe children should not be targeted with personalised advertising. But further research into the overall prohibition of (online) advertising to children could be beneficial.

Second: we already discussed the inclusion of children in user panels, to promote more comprehensible privacy policies. This inclusion could be taken a step further in the form of an obligation to include children in Data Protection Impact Assessments (DPIAs). Most social media platforms will be required to perform a DPIA, as they process data on a large scale, and from vulnerable data subjects, two criteria that are likely to result in a high risk, and therefore warrant a DPIA, according to the WP29.<sup>33</sup>

32 Ingrida Milkaite & Eva Lievens (2019): Child-friendly transparency of data processing in the EU: from legal requirements to platform policies, Journal of Children and Media, p. 13 <https://doi.org/10.1080/17482798.2019.1701055>

33 WP29, 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, p. 10.

# Annex I

We have examined the conditions of use and privacy statements of the largest social media platforms: TikTok, Facebook/Instagram, YouTube and Snapchat. In this examination, we focused on the process of requesting consent, whether children's data are handled any differently, and the clarity of the privacy statement. In addition to our own interpretation regarding clarity, we also used readability checkers, which can be found at <https://sitechecker.pro/readability-checker/> and <https://www.webfx.com/tools/read-able/>.

## 3.1 TikTok

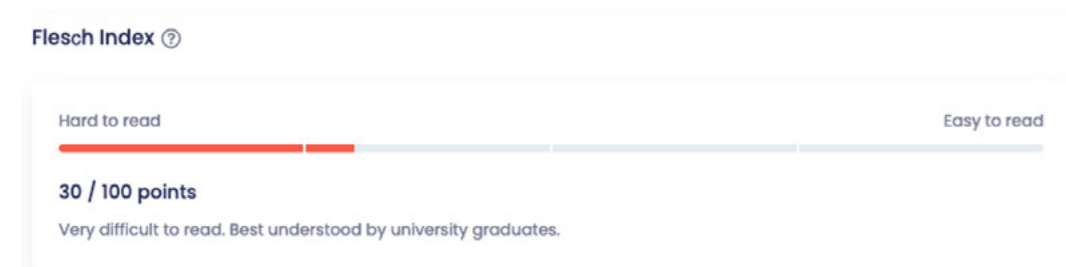
At the bottom of the login screen, before you choose which medium you want to use to log in (mail, telephone number, Facebook, Google, Twitter), it says in small letters that you agree with the terms of use and the privacy statement. Because of the position on the screen and the absence of a pop-up, it is easy to gloss over this. Therefore, children will not be informed or actively asked for their consent. You have to fill in your date of birth, but this will not be checked. Even if you fill in at age 13, you will not get an informative pop-up and you can start scrolling right away. It is difficult to see in the preferences whether you can disable personalised settings.

However, according to the privacy statement, data of younger users are simply used for personalised content and contextual advertising, although data of younger users are not sold to third parties - it remains unclear whether data of users aged thirteen or older are sold to third parties. There is an opt-out option for personalised advertisements.

TikTok is the only one of the platforms surveyed that has a separate [privacy statement](#) for children. In addition, there are special measures for users under the age of thirteen. They can watch and make films, but they cannot make them public on the TikTok platform. Children under the age of thirteen cannot send messages either, and their profile is not visible to others. The privacy statement for EEA residents and the privacy statement for younger users are fairly clear, but especially for younger users, they become very formal, legal and long.

The readability checkers use the 'Flesch Index', a popular formula to measure the comprehensibility of a text. Texts written for marketing purposes should score no lower than 70%. Figure 1 shows that TikTok scores 30%, qualifying it as a text at university level. Since this privacy statement is aimed at younger users, it cannot be said that clear and simple language is being used, which could constitute a breach of article 12 GDPR.

Figure 1: Readability Checker - TikTok Privacy Policy for Younger Users



## 3.2 Facebook / Instagram

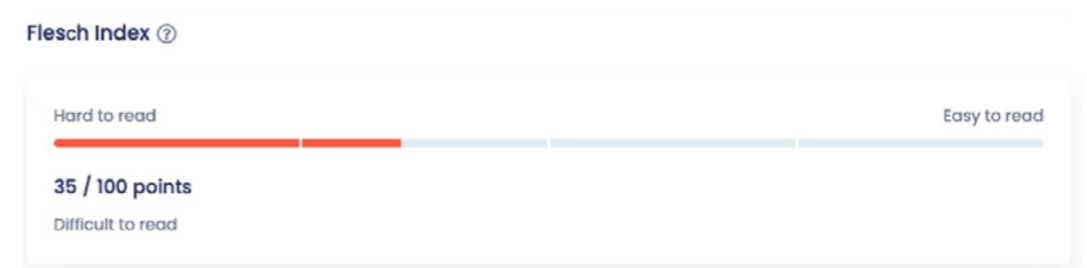
Since Facebook's [data policy](#) also applies to Instagram, both services have been considered in this analysis. WhatsApp has not been taken into account. However, we have noted that the minimum age for WhatsApp is 16 years. On the other hand, the minimum age for Facebook and Instagram is 13 years. Children between the ages of 13 and 16 have to get permission from a parent, the parents can give this permission through their own Facebook account. With Instagram it works slightly different, unless an Instagram account is created with a Facebook login. In the case of a stand-alone account, the parent must give permission by sending an ID copy or by completing a one-time credit card payment. If the parent does not do this, the child will be given a restricted version of Instagram, where the child will not be able to make the profile public.

Although parents might find this an even better option, this in turn poses a risk of circumvention. Children evidently need the opportunity to make their profile public, and may inadvertently share more data than they think. For example, a recent study by the Irish Data Protection Authority showed that children had converted their personal profiles to a business profile in order to see statistics. However, this also meant that the children's telephone number and e-mail address were made public. The investigator who discovered this error estimates that five million children have been affected.<sup>34</sup> Although Facebook states that it has clearly stated that contact details are made visible in business profiles, it is clear that this feature should not have been available to children.

Furthermore, there is nothing unexpected in the privacy policy. No distinction is made between adult and younger users, so profiles are also created about children to create personalised advertisements.

In this privacy statement, the two readability checkers we used disagree with one another. One gives Facebook a low score (35%), the other says it is very readable, even for children (65%). Since even the high score is below 70% - the lower limit for marketing texts - and the data policy is 19 pages long, we conclude that Facebook's privacy statement is partly unclear, but in any case not concise, especially if it should be read by a child.

Figure 2: Readability Checker - Facebook and Instagram Data Policy



34 <https://www.telegraph.co.uk/technology/2020/10/18/instagram-investigation-exposing-millions-childrens-contact/>

### 3.3 YouTube

To create your own YouTube channel, you need a Google account. In its [privacy policy](#) Google uses an age of 16 years. A child younger than this age must have permission from his or her parents. In order to create an account, a parent's email address is first requested in order to grant this permission.

For the processing conditions, YouTube refers to the Google terms and conditions. In particular, it states that the collection of personal data is used to provide better services to users. In the case of YouTube, this will be suggestions for a YouTube video. This suggestion is made on the basis of the collection of activity-related data, such as terms searched for, viewed videos, but also the browsing history on Google Chrome, or on the basis of activities on third party sites and apps that use the Google service.

In addition to video suggestions, data from YouTube are also processed for personalised advertisements. For example, a child watching videos from guitar players will see advertisements for guitars or guitar lessons. For these personalised advertisements Google / YouTube asks for permission. Permission from parents for their children is already included in the permission to create an account.

The fact that no distinction is made between personal data of children and adults also means that personalised advertising is created for children. Only in the YouTube Kids app is it forbidden to offer personalised advertisements. Only data are processed for personalised content. However, this app is aimed more at a younger target group (from 4 to 12 years of age). Children between the ages of 8 and 16 will mainly be on the regular YouTube platform.

The personal data of children will not be handled differently than the personal data of adults. As a result, no distinction is made in the terms of use and privacy policy. As stated in section 2.1 of this report, there must be clear and simple language when processing is specifically aimed at a child. A whole piece of text will not be easily read by a child. However, Google does use short films with visualisation. Google does not use any part specifically aimed at children.

Here again, the readability checkers vary somewhat. One gives a score of 34%, while the other gives a score of 52%. As with the previous platforms, Google does not score particularly high. Since this statement counts 30 pages, it is not realistic that children will read it. Youtube Kids, which is specifically aimed at children, would benefit from having a separate, simplified privacy statement.

Figure 3: Readability Checker - Google Privacy Policy



### 3.4 Snapchat

Snapchat has a minimum age of 13 years. Parental consent is not required when creating a child profile (if an age below 16 is filled in). In view of article 8 paragraph 1 AVG, this means that no data may be processed for personalised advertising. This is somewhat stated in their [privacy statement](#):

***“Our services are not intended for—and we don’t direct them to—anyone under 13. And that’s why we do not knowingly collect personal information from anyone under 13. In addition, we may limit how we collect, use, and store some of the information of EU users between 13 and 16. In some cases, this means we will be unable to provide certain functionality to these users. If we need to rely on consent as a legal basis for processing your information and your country requires consent from a parent, we may require your parent’s consent before we collect and use that information.”***

Interestingly, it seems that this is actually being done. A child profile can be created without the parent's consent. In this case, the data processed are based on activities (i.e. personalised), unless you disable this. Instead, it should be turned off, unless permission is requested from a parent. Snapchat does not comply with the GDPR in this case.

It is also relevant that data are processed from the camera and photos, about the number of messages you exchange and about log data. Another interesting point is the collection of location details. Consent must be obtained for this. This is mentioned in their privacy statement. It states that location information is used to label the content of your Memories (a personal collection of Snaps and Stories that you have saved) and to offer and improve advertisements. The privacy policy also states that consent will be requested before this information can be used for this purpose. Parental consent is also not obtained here. It should therefore not be possible to offer personalised advertisements with this location information. The question is whether this has actually not been done.

At Snapchat, the readability checkers are more in agreement with each other, with a score of 44 and 54 percent. The privacy statement is 15 pages long, which is still quite a bit of text for children. Snapchat does not have a privacy policy specifically aimed at children.

Figure 4: Readability Checker - Snapchat Privacy Policy



# Justification

The Hague, February, 2021

This position paper has been written on behalf of the Dutch Consumentenbond. This position paper reflects the recommendations and conclusions of the Consumentenbond and of the authors of the ILP Lab. This paper has benefited from the input of the following experts: Gerrit-Jan Zwenne from Pels Rijcken, Eva Lievens from UGent, Justine Pardoën from Bureau Jeugd en Media, Bernice Samson from Centrum voor Jeugd en Gezin, David Martin from BEUC and Ot van Daalen from IViR.

Authors of the ILP Lab: Dorine Dollekamp and Tommy Fitzsimons of [the Glushko & Samuelson Information Law and Policy Lab](#) (ILP Lab) of [the Institute for Information Law \(IViR\)](#) of the University of Amsterdam. The ILP Lab is a student-run, IViR-led institution which develops and promotes research-based policy solutions that protect fundamental rights and freedoms in the field of European information law.

## Contact

Consumentenbond  
Enthovenplein 1  
Postbus 1000  
2500 BA Den Haag  
Telefoon 070 445 45 45  
[consumentenbond.nl](http://consumentenbond.nl)