D2.3 Methods for obtaining parental consent and maintaining children rights

Hof, S. van der; Ouburg, S.

Project Number: LC-01622116 / 101018061
Project Acronym: euConsent

Project title: Electronic Identification and Trust Services for Children in Europe

Project Programme: Project Programme: PPPA-AGEVER-01-2020: "Outline and trial an infrastructure dedicated to the implementation of child rights and protection mechanisms in the online domain"

Methods for Obtaining Parental Consent and Maintaining Children Rights

WP2: Existing Methods, User Needs and Requirements

Date: 25/06/2021

Doc. Version: 01

Authors: **Prof. Simone van der Hof and Sanne Ouburg**
Partner: **Leiden University**

Document Control Information

Settings	Value
Document Title:	**Methods for Obtaining Parental Consent and Maintaining Children Rights**
Document for:	**WP2: Existing Methods, User Needs and Requirements**
Project Title:	**Electronic Identification and Trust Services for Children in Europe**
Document Author:	**Prof. Simone van der Hof and Sanne Ouburg**
Partners:	**Leiden University**
Doc. Version:	**01**
Date:	**25/06/2021**

Document Approver(s) and Reviewer(s):

Name	Partner	Role	Action	Date
			<Approve / Review>	
Abhilash Nair	**Aston**	**Reviewer**	**Review and approve**	**24 June 2021**
Sonia Livingstone	**LSE**	**Reviewer**	**Review and approve**	**25 June 2021**

Document history:

Revision	Date	Created by	Short Description of Changes
version 01	**25 June 2021**	**Simone van der Hof & Sanne Ouburg**	**N/A**

Table of contents

1. Executive summary

This study has mapped existing methods for age verification and obtaining parental (or guardian) consent in various digital services (such as apps and games) that are used by children. Moreover, we have assessed how the age verification and parental consent methods in these digital services that we have identified can be assessed based on the data protection and children's rights framework.

The purpose of this study was not to do a full compliance check on what methods are used and how they have been implemented but to determine how they comply with the directly relevant provisions in the GDPR, including Article 8 GDPR on parental consent. Furthermore, we did examine how the methods relate to the principles of data minimisation and privacy by design, given that these are particularly relevant to the protection of children.

The children's rights analysis shows how the rights of the child as enshrined in the 1989 UN Convention on the Rights of the Child which are relevant to the design, development and use of apps and games used by children, trigger specific considerations with respect to the age verification and parental consent methods identified in the apps and games.

Our most important findings are:

- ## Most apps and games use self-declaration as the method for age verification

The method most commonly used for age verification is self-declaration. Clearly, this method makes it easy for the user to manipulate age verification (and, hence, circumvent parental consent if it is even present in cases where it was required). There is an incentive for children under 13 (or the applicable age of digital consent) to claim to be older than the minimum age to sign up for digital services; otherwise they will be excluded from most services. Even where a potentially more effective method was implemented, age verification could still be circumvented. The lack of adequate age verification also (i.e. digital services do not verify who is a child, a person under 18) also means that the protection of children cannot be taken into account more generally when processing their personal data.

- ## If age verification is circumvented, consent is potentially unlawful

Since age verification can be easily circumvented, there is a high probability that children who have not yet reached the age of digital consent will consent to their data being processed, as a result of which, consent is unlawful. Either digital service providers must implement more appropriate age verification or they should not process children's personal

data where consent is required. Given that data processing for which consent is required often involves data-driven processing practices (e.g. personalised advertising), the option to not process personal data of children in those instances is preferred.

- ## If a method for parental consent is present then it is mostly based on self-declaration

Parental consent mechanisms of digital service providers are mostly based on self-declaration as well, with the child, for example, being asked to provide an email address of the parent (or guardian) who must then respond by giving the child permission to open an account. Although some services indicate that they ask for parental consent or have special settings for children under 13, we could not always find a parental consent mechanism. Where parental consent was requested (e.g. by linking the child's account to that of the parent), it was not actually verified as being the parent (or guardian). We found one exception though, where copies of official documents had to be provided to prove the parent's identity as well as parental authority or guardianship. This clearly provides a higher level of assurance but using copies of official documents is not necessarily the most privacy-friendly method.

- ## Self-declaration is not an adequate verification method for high-risk data processing

The adequacy of the verification method depends on the risks involved in the processing of personal data. When determining the risk of data processing, the following factors must be considered: the vulnerability of the person whose personal data is involved, the types and sensitivity of data being processed, the type of service that processes the data, accessibility of data by and sharing of data with others. From a data protection perspective, at low risk, a method that is not watertight will suffice, such as asking the user whether they are under or over a certain age (self-declaration). Also, if a person claims to be a child (under 18) or under the age of digital consent, you may assume this to be true and apply specific data protection for children. However, we recommend that the processing of personal data of children, a group explicitly designated as vulnerable by the GDPR, be classified as high risk. Especially if that processing serves commercial purposes and offers the possibility of personalisation based on behavioral data and profiling.

- ## Parental consent (if asked) is often not designed as specific consent

For consent to be lawfully given it must be specific consent. Agreeing to a privacy policy is, as a rule, not specific consent but this was still the most common way in which parents were asked for consent. Specific parental consent requires that parents give their

consent to data processing for a specific purpose. They must also have a clear choice to say yes or no and, moreover, consent must be withdrawn as easily as it is given. Neither is the case if the only option is to agree to the privacy statement in order to use the app or game.

- ## Privacy settings allow parents to provide specific consent

Some digital services offered parents the option to say yes or no when the child wanted to adjust the privacy settings in their account. If this is designed in an understandable and accessible way and the parent (and preferably also the child) is immediately provided with sufficient information about the specific data processing, this can be a good option for legitimately obtaining *specific* parental consent. This way the parent has a choice and consent can be withdrawn as easily as it is given if the privacy setting can be easily reset in the same way.

- ## Parental consent is not the same as parental control

Parental consent is not to be intended as a tool for parental control over the actions of children when they use apps and games. Parental consent is a legal act of consenting to data processing for a specific purpose which makes the data processing lawful. Parents must make this decision for their children when they are under a certain age, based on the idea that they will better understand the consequences and risks of certain data processing operations. This requires parents to gain insight into the what, how and why of specific data processing by the digital service provider, but not also into how a child uses their account or their other online activities. Parental control covers a range of tools or strategies to guarantee the safety of children beyond data processing and can be used at the discretion of parents (but preferably in open communication with their children).

- ## Verification methods must be privacy-preserving

In the design and development of verification methods, the principles of data minimisation, privacy by design and privacy by default should be central. This includes, but also goes beyond, the principle of data minimisation, on the basis of which only necessary and (also sufficient) personal data are processed in order to carry out adequate verification. It goes beyond data minimisation because other data protection principles and rights must also be implemented by design. The principles of privacy by design and privacy by default require that verification methods must also take into account the protection of children (i.e. persons under 18) and their personal data specifically by designing them in a child-friendly way that is transparent and accessible to them and allows them to exercise their rights quickly and effectively. Specific privacy by design strategies include anonymization and pseudonymization as well as the use of decentralised, open source solutions.

In the case of age verification, it is only necessary to know whether a person is 18 or over or over the age of digital consent when consent is one of the lawful grounds. If a person indicates by self-declaration to be a child (under 18) then no further verification needs to take place and it should be assumed that the specific protection of children under the GDPR applies. Also, in case consent is the lawful ground, if someone indicates by self-declaration that they are under the age of digital consent, it can be assumed without further verification that parental consent is required. When verifying parental consent, it is only necessary to know whether or not someone is the parent (or if difficult to determine: potentially only whether someone is an adult). When verification took place, most digital services asked for official documents (ID, birth certificate), which show more information than necessary.

We discourage verification methods that use sensitive personal data or automated profiling, unless it is demonstrably in the best interests of the child and age appropriate safeguards are in place. Furthermore, the verification process should preferably take place on the child's or parent's device rather than at the digital service provider or a third party verification service provider to avoid the creation of, potentially large, central databases that may be vulnerable to external attacks and other data breaches.

Personal data of children collected by verification methods should not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

- ### Verification methods must be sensitive to the privacy expectations of children in relation to their parents

Child-friendly and privacy-preserving verification methods must also take into account children's privacy expectations towards their parents. Especially for teenagers, it is expected to be important that parental consent does not also mean that parents can look into their account or into their online activities, some of which may be sensitive, intimate or just intended to be seen by peers or best friends. For younger children, this may be different and parents may want to be more involved in keeping an eye on their children's safety (for example, by using parental control tools). In order to make the distinction, it is important to make a clear separation between parental consent mechanisms and parental control tools. Preferably the privacy settings for parental consent mechanisms take into account that children may want to limit what parents can see to the data processing for which consent is given and are otherwise private by default. Parental control tools should be built in if necessary with the evolving capacities of children as a guiding principle.

- ### Verification methods must be transparent

The operation of verification methods must be accessible and understandable to children. This means, among other things, that it must be clear to children which personal data is processed in which way in order to verify their age and, if necessary, the consent of their parents. We noticed, for example, that some digital services automatically determined whether we met the minimum age of digital consent of the country from which we signed up, which implies that location data is being processed. However, we could not find any information about this. It should also be transparent to children what parents (or guardians) can see in relation to their account when giving consent. Verification methods should be offered in the child's language. Finally, transparency of verification methods is a constant point of attention. Especially if adjustments are made to these methods, it must be clear that the process is still transparent to children and their parents.

- ### The best interest of the child must have priority when designing verification methods

The best interests of the child, a fundamental principle in the 1989 UN Convention on the Rights of the Child, should always be the starting point when an activity has an impact on children. This applies also to the verification methods used or to be designed and developed. It should be borne in mind that digital services can make a hugely important contribution to children's development and should therefore be accessible to children and excluding them is not necessarily in their best interest. At the same time, providers must ensure that their digital services do not have a harmful impact on children. The design of the technologies will therefore have to take into account the realisation of a positive contribution to children's development and the prevention of harmful effects on them which is also true for verification methods. The best interests of the child can be implemented - together with the other rights of children - by carrying out a child rights impact assessment.

- ### Children and their parents must be involved when designing and developing verification methods

When designing and developing verification methods, it is important to involve children and parents so that their views, experiences, needs and wishes can be taken into account. Children will need to be involved in some way in the design, development and testing of verification methods as these impact on their use of digital services. Particularly, children must be consulted on the age appropriate nature of digital services and any age gating for the purposes of their protection. Moreover, the choices made in the design process of verification methods may have an impact on their (other) rights, including their best interests, which makes involving children important as well. Therefore, when carrying out a children's rights impact assessment, it is also essential to include the views of children, and preferably also their parents.

- Verification methods must take into account the evolving capacities of the child

Children are all persons under the age of 18, but groups of children and individual children can be very different from each other, given their age and specific stage of development. Design and development must therefore take into account that what is accessible and understandable for some children may not be for others and ensure that methods are usable by all children concerned.

- Verification methods must be inclusive

Verification methods must be inclusive and children (or their parents) should not be excluded because they cannot meet the requirements set by the verification methods. A child rights impact assessment must identify the issues that may arise with regard to inclusiveness and how to prevent them. Here it may be relevant, for example, that children or parents may not have access to certain verification methods (e.g. eID or credit card) or that it is complicated in the personal context of the child to ask for parental consent. Particular attention should be paid to making digital services (including age verification and parental consent mechanisms) accessible to children who face specific challenges such as physical and intellectual disabilities.

- Effective and child-friendly support and remedies must be implemented

Children must be offered accessible and effective age-appropriate instruments to enable them to make complaints when their interests or rights are not observed or get support in using verification methods.

- Conducting a child rights impact assessment is strongly advised when designing verification methods

It is strongly advised to perform a child rights impact assessment to determine how verification methods may impact children and children's rights and assess how to implement legal requirements and address any concerns by implementing age appropriate safeguards. This should prevent the situation in which GDPR compliance drives the design and development of parental consent and age verification methods and ensure that the rights of children are also taken into account. It is essential to involve children and parents in the process because they themselves are best placed to indicate their experiences and expectations. Moreover, an impact assessment is not a one-off exercise because the consequences of using verification methods and new technological developments may require adjustments.

2. Acknowledgements

We thank our project partners in the euCONSENT consortium for their wonderful cooperation. We especially thank the members of WP2 for their great support and the many extremely inspiring and helpful discussions we had with each other during the research.

Special thanks go to Abhilash Nair (Aston University), Sonia Livingstone, Mariya Stoilova (both London School of Economics and Political Science), Tony van Rooij (Trimbos Institute) and Bart Schermer and Bart Custers (both Leiden University) for reviewing our work and providing valuable suggestions.

3. Glossary of key terms

Age assurance: An umbrella term for methods used to determine the age or age-range of an individual to varying levels of confidence. There are three principal categories of Age Assurance methods; age verification, age estimation and self-declaration The word 'assurance' also refers to the varying levels of certainty that different solutions offer in establishing an age or age range which is influenced by which of these three types of method is applied.

Age verification: verification of the age of a data subject in order to determine whether they are a child or have reached the age of digital consent.

Biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (Article 4 (14) GDPR).

Child: a natural person below the age of eighteen years (Article 1 CRC).

Children's consent: consent given by a person under the age of 18 who has reached the age of digital consent pursuant to Article 8 GDPR.

Consent: 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Article 4 (11) GDPR).

Consent mechanism: a method of obtaining consent of the data subject.

(Data) controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4 (7) GDPR).

(Data) processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4 (8) GDPR).

Data subject: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 (1) GDPR).

Information society service: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (Article 4 (25) GDPR and point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council).

Joint consent: consent jointly given by a person who has not yet reached the age of digital consent and the holder of parental responsibility over that person.

Parental consent: consent given or authorised by the holder of parental responsibility over the child pursuant to Article 8 GDPR.

Parental control (tool): a tool that can be used by parents to monitor the safety of their children.

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 (1) GDPR).

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4 (2) GDPR).

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4 (4) GDPR).

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4 (5) GDPR).

Self-declaration: A method of age assurance which relies on the individual to supply their age or confirm their age-range. This method establishes age or age-range to a very low level of assurance. It may be fit-for-purpose in some contexts. The level of assurance can be slightly increased through the design of the self-declaration process. Self-declaration can be used in combination with other methods e.g. age estimation to provide a higher level of assurance.

4. Introduction

This work is part of an EU-funded project euCONSENT which aims to put into live operation a pan-European open-system for age verification and parental consent which is secure, certified, and interoperable and proposes measures that respect, protect, and remedy children's rights in the digital age (UN, 2021). This review is part of a working group on existing methods, user needs and requirements responsible for:

- Conducting research on the existing laws and regulations in the EU (see Caglar and Nair, 2021).
- Reviewing methods for obtaining parental consent and maintaining children rights (this report).
- Studying the EU methods for compliance with the Audiovisual Media Services Directive (AVMSD) and General Data Protection Regulation (GDPR) (see Billinge et al., 2021).
- Carrying out a rapid review of the existing evidence on age assurance and parental controls from the perspective of children and families (see Smirnova et al. 2021).
- Conducting a qualitative study on the views of EU children on online protection systems (forthcoming).

The results of this work package will feed into the forthcoming technical work making sure that the measures proposed by euCONSENT respond to the needs and expectation of all involved users and related stakeholders, also taking into consideration the currently established methods and practices, as well as legal and ethical factors.

4.1. Objective and definition of research

This study aims to map existing methods for obtaining parental (or guardian) consent and identify how they comply with the relevant substantive data protection framework applicable in EU Member States, including specific data protection principles, i.e. data minimisation, privacy by design and privacy by default, as well as the best interests of the child and other children's rights in the UN Convention on the rights of the child.

Although we will examine to some extent how companies have legally structured their data processing, particularly to determine whether consent is used as lawful ground, it is not within the scope of the study to analyse the extent to which apps and games comply with data protection legislation. Also, the child rights analysis will only focus on the consent mechanisms used in apps and games that are likely to be used by children and will not address the broader issue of whether the commercial and data practices used by digital service providers or the design of apps complies with children's rights. Age verification is inextricably linked with children's and parental consent given that the GDPR holds an implicit age verification obligation to determine whether under 18s are using a digital service (for the purpose of applying data protection in a child appropriate way) and if and when consent is the lawful ground for personal data processing, whether under 16s (or the applicable age of digital consent) are using a digital service (for the purpose of applying Article 8 GDPR and related national implementation provisions on parental consent). Age verification in relation to the GDPR is therefore also part of the study.

The questions addressed in this study are:

- What methods are used for age verification and to obtain parental consent?
- How do these methods comply with data protection laws?
- How do these methods comply with children's rights?

4.2. Methodology

The study combines (1) desk research into (a) the legal requirements for age verification and parental consent under the GDPR, (b) the extent to which the age verification and consent mechanisms in selected apps and games comply with these requirements, and (c) the extent to which the consent mechanisms in selected apps and

games comply with children's rights and (2) case study research into consent mechanisms used in a selection of apps and games

(1) (a) This part of the study will explain the legal regulation of consent under the GDPR and particularly the conditions for consent by children and parents. Moreover, it will explain the principles of data minimisation and privacy by design in relation to consent. (b) The findings from the mapping under (2) will be analysed based on the legal requirements for consent mechanisms under the GDPR. (c) This part of the study will first make a more general analysis of relevant children's rights in relation to consent under the GDPR. The insights from this part of the study are then applied to the results of the study under (2). Part (1) will be based on desk research.

(2) The study maps parental consent mechanisms in selected apps and games (likely to be) used by children. The selection is made from apps and games that are popular among children and young people. The popularity is based as much as possible on evidence but will sometimes be based on best guess choices because data is not always available. In the case of games, an initial exploration shows that there is no data on the most popular games among children. We will also include some lesser known and/or popular apps that are probably also used by children. After the selection of apps and games, a mapping is made on various aspects related to consent mechanisms. For this purpose, an analytical framework is developed based on (1) that examines whether consent is a lawful ground for data processing in each of the apps and whether and how it is ensured that parents consent in cases where this is required by law. In this analysis, we also take into account whether the principle of data minimisation, i.e. personal data is only processed when absolutely necessary for the verification of age and parental consent, is met. We will not do a full compliance check and the question whether all conditions for consent are met (such as: is consent the most appropriate legal basis, is the purpose limitation principle met, is there informed consent, is there free choice?) are beyond the scope of the study. When apps and games exclude children of a certain age in their terms and conditions but there is no (significant or effective) age verification, we assume that for children under a given age as defined in Article 8 of the GDPR (as well as EU member state laws implementing Article 8 of the GDPR) parental consent must be given for personal data processing for which consent is the lawful ground (Article 6 (1) (a) GDPR). We include in the analysis whether options are provided to allow guardians other than the parents to give parental consent. In applying the analytical framework, we look at the method of signing up for an app or game and also the settings associated with an account. For the latter, we analyse to what extent parents can consent to privacy settings in view of the processing of children's personal data in the child's account.

4.3. Approach

The research starts with a data protection and children's rights analysis of consent to determine the legal requirements for children's and parental consent for data processing by digital services (section 5). Section 6 then provides an analysis and assessment of the mapping of age verification and consent mechanisms in apps and games (see Annex 1 for the latter). This part of the study answers the research questions: What methods are used for age verification and to obtain parental consent?, How do these methods comply with data protection laws? and How do these methods comply with children's rights? Section 7 wraps up this study with conclusions.

5. Consent and age verification under the GDPR

5.1. Introduction

This chapter explains consent as one of six lawful grounds under the GDPR (section 5.2.1.) and particularly focuses on both the situation in which children have reached the age of consent (section 5.2.2.) and in which they have not reached the age of digital consent (section 5.2.3.) as well as verification of parental consent (section 5.2.4.). Moreover, this chapter explains the requirements of age verification (section 5.3.) and the principle of data minimization which needs to be observed when building and implementing verification methods (section 5.4.). The chapter wraps up with an analysis of consent and age verification from a children's rights perspective (section 5.5.).

5.2. Consent

5.2.1. Consent as a lawful ground under the GDPR

Consent is one of the lawful grounds in the GDPR (Article 6 (1) (a) GDPR). A lawful ground is one of the conditions for the processing of personal data to be lawful. The most common lawful grounds for apps and games are consent, necessary for the performance of a contract (Article 6 (1) (b) GDPR) and legitimate interest (Article 6 (1) (f) GDPR). In principle, it is first examined whether there is a suitable lawful ground other than consent for the processing of personal data. If this is not the case, then consent can be used as a lawful ground. For consent to be lawful, it must comply with the conditions of Article 7 of the GDPR, which entail that consent is informed, freely given, unambiguous, can be withdrawn

as easily as it was given and the controller must be able to demonstrate that the data subject has consented to the data processing.

When personal data of children under the age of digital consent is processed by information society service providers (hereafter digital service providers) and consent is the lawful ground for a specific processing purpose then the conditions of Article 8 GDPR must be complied with as well. Article 8 applies when the company provides an information society service (see section 3.). Apps and games analysed in this study all qualify as information society services. Moreover, the information society service must be offered directly to a child (Article 8 (1) GDPR). If a digital service is solely aimed at adults and there is no evidence to the contrary (including content and marketing plans), then Article 8 GDPR does not apply to a digital service because it will not be considered to be 'offered directly to a child' (European Data Protection Board 2020).

This study focuses exclusively on consent, but it should be noted that also the lawful grounds 'necessary for the performance of a contract' and 'legitimate interest' raise specific questions with regard to children (i.e. persons under 18). In the case of 'necessary for the performance of a contract', there must be a legally valid contract. Whether children have legal capacity to conclude a contract depends on the applicable contract law. It is likely that parents will have to give their permission if their children conclude a contract. In the absence of such permission, the agreement may be void or voidable. This is a different form of consent from that referred to in Article 8 GDPR which will be the focus of this study (see also Article 8 (3) GDPR). Article 8 GDPR deals exclusively with consent in relation to the processing of personal data.

Children are not always legally entitled to consent to the processing of their personal data. The reason is that children are not always (depending e.g. on age or cognitive abilities) likely to fully understand the risks and consequences of data processing and what rights they have in this regard and how to exercise them (see Recital 38 GDPR). For this reason, Article 8 GDPR stipulates that in the case of children under a certain age, parental consent is required for the processing of their personal data by commercial digital services. Above that age, children have reached the age of digital consent and can give their own consent. The next two sections elaborate on each of these situations.

5.2.2. The child has reached the age of digital consent[1]

The general rule is that children of 16 and older have reached the age of digital consent and for children under 16 parental consent is required. However, EU Member States

[1] Note that the age of digital consent refers specifically to the age when a child can consent to data processing and should not be understood as an age when children are allowed to use social media.

have a discretionary power to provide in their implementing legislation that children under 16 can give their own consent to data processing, as long as they are not under 13. This has led to very different age ranges across the EU (Milkaite and Lievens, 2019) and the European Commission is now investigating whether the age can be harmonised (European Commission 2020). Companies are playing it safe by choosing 16 when developing their services because in that way they always meet the requirements of the GDPR, irrespective of national implementations of Article 8 GDPR. From a child rights perspective, though, this may not be the most appropriate or at least most desirable age given that children can consider it an invasion of their privacy when parents are required to consent to their online activities (see section 5.5.3.2.).

When a child reaches the age of digital consent after consent was initially given by the parent, parental consent nevertheless remains valid. However, the child may withdraw such consent on the basis of Article 7 (3) GDPR. Consent can also be withdrawn to trigger the right to erasure (see Article 17 (1) (b) GDPR), a right that is considered particularly important for children (Recital 63 GDPR). The provider of the digital service must inform the child of these possibilities (European Data Protection Board 2020, nr. 149).

For consent given by a child that has reached the age of digital consent to be valid, it must be understandable to the child concerned what they are consenting to (i.e. consent must be informed) (also see Article 12 GDPR). However, many privacy policies are likely to be below the level of understanding of an under 18 (Commission Nationale de l'Informatique et des Libertés (CNIL) 2020), in which case consent is not informed. Furthermore, agreeing to a privacy policy is, as a rule, not specific consent. Data subjects must be confronted with a clear choice for a specific data processing, after which they can consent (i.e. agreeing with the particular option through an affirmative action) in order to meet the requirements for valid consent.

5.2.3. The child has not reached the age of digital consent

When children are under the age of digital consent, the holder of parental responsibility needs to consent on behalf of their children if consent is the lawful ground (Article 6 (1) (a) and Article 8 (1) GDPR). The holder of parental responsibility will by default be the parent of the child. However, the person responsible for a child can also be someone else and several persons (natural or legal) can be responsible for a child.

It is interesting that in France, joint consent by the parent and the child who has not yet reached the age of digital consent is required.[2] Based on the provision concerned, the age

[2] Article 45 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés provides: *"En application du 1 de l'Article 8 du règlement (UE) 2016/679 du 27 avril 2016, un mineur peut consentir seul à un*

for consent to the processing of personal data regarding the offer of information society services is 15 years old. When a person is under 15, any processing of personal data of that person based on consent is only lawful when consent is given jointly by that person under 15 and the parent, or any other person that holds parental authority with respect to the child concerned.[3] Incidentally, national implementing legislation is not supposed to go beyond what is provided for in the GDPR (European Commission 2020), but it appears that the French legislators have followed their own interpretation of consent, deviating from the GDPR.

Though this has not found its way to Article 8 GDPR,[4] parental consent is not considered to be required for preventive or counselling services provided online (Recital 38 GDPR; (European Data Protection Board 2020, nr. 150; see also Committee on the Rights of the Child 2021; Committee on the Rights of the Child 2016). Examples for such exempt services could include online child helplines such as those offered by organizations affiliated to Child Help International.

5.2.4. Verification of parental consent

The verification of parental consent may not always be easy to achieve given that it may be difficult to determine with reasonable certainty who has parental responsibility. What is a reasonable method may change with the development of new technologies (European Data Protection Board 2020, nr. 146) or depend on the context (e.g. there is a registration of parental authority in a Member State that can be used in the verification process). In any case, 'available technology' must be used pursuant to Article 8 GDPR, which means that technological developments in verification methods must be monitored by digital service providers (Data Protection Commission Ireland 2020, also giving examples of methods in section 5.2.).

Alternative methods are worth considering when verifying parental consent is difficult (e.g. allowing a person over 18 to consent on behalf of the child or a person over 18 years of age with a reasonable age difference from the child potentially allowing them to be their parent), although it is not entirely clear whether this complies with the GDPR. It can be

traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans. Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur. [...]"

[3] See also D2.4. on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 28, children consider it important to be involved in mediation decisions. Although consent is a legal act that in this case must be performed by both parent and child, the concept of joint consent creates opportunities for shared decisions and open communication about choices.

[4] See, however, Article 9 (b) UK Data Protection Act 2018, which exempts preventive or counselling services from information society services.

argued that it is sufficient if someone consents who - like the parent - has a better understanding of data processing than the child, given that this is the particular concern mentioned in Recital 38 of the GDPR. Article 8 GDPR is not intended to be a tool for parental control over the actions of children when they use apps and games. However, parents are primarily responsible for their children (Article 18 CRC) and they may want to have a say in data processing given its potentially high-risk nature in many apps and games.

The choice of a parental verification method also depends on the risk involved in the processing of personal data (see also section 5.3. on age verification). An email may be sufficient proof in low-risk cases, but high risk data processing is likely to require more reliable proof. A method mentioned by the EDPB in that case is making a bank or credit card payment of €0,01 by the holder of parental responsibility explicitly stating that they are indeed the holder of parental responsibility over the child (European Data Protection Board 2020, fn 68). In line with what was said in the previous paragraph about the difficulty of establishing that someone is the child's parent, in low-risk situations the choice could be made to ask the consent of an adult who, given their age, could be the parent. The verification of parental consent may also be outsourced to trusted third parties (European Data Protection Board 2020, nr. 137).

Any method for verifying parental consent that processes personal data must itself comply with the GDPR and more specifically be transparent (Articles 5 (a) and 12 et seq. GDPR) and privacy preserving (Articles 5 (c) and 25 GDPR; see section 5.4. on privacy by design).

5.3. Age verification[5]

Age verification is an implicit requirement in the GDPR given that children need to be awarded special protection given their particular vulnerabilities (Recital 38 GDPR) (Van der Hof, Lievens, and Milkaite 2019; Data Protection Commission Ireland 2020). It is therefore important to know whether children (persons under 18) use a digital service, regardless of whether Article 8 GDPR applies (Data Protection Commission Ireland 2020). The alternative is for digital services to be designed age-appropriate by default so that age verification is no longer necessary (5Rights Foundation 2021). More specifically, this means eliminating privacy-invading data processing which generally requires consent (as it is not likely to be a legitimate interest of the digital service provider that overrides the child's rights and interests, (Article 6 (f) GDPR)) and may trigger the application of Article 8 GDPR on children's age of digital consent.

[5] See for examples of age verification methods, Nash et al. 2013; Van der Maelen 2019; ICO 2020; Data Protection Commission Ireland 2020; UNICEF 2021; 5Rights Foundation 2021. See also D2.2 EU Methods for AVMSD and GDPR Compliance Report for an overview of age verification methods.

In case Article 8 GDPR applies (i.e. consent is the lawful ground) reasonable efforts must be made to adequately verify that a user has indeed reached the age of digital consent if they claim to be above a certain age (e.g. over 16 if that is the age of digital consent). This is important because data processing is unlawful if consent is given by a child who has not yet reached the age of digital consent (European Data Protection Board 2020, nr. 133). If the user indicates that they have not yet reached the age of digital consent, the truth of this statement does not need to be verified. In that case, parental consent can be assumed to be required (European Data Protection Board 2020, nr. 134).

Moreover, if a service is solely aimed at adults and there is no evidence to the contrary (including content and marketing plans), then Article 8 GDPR does not apply to a digital service because it will not be considered to be 'offered directly to a child' (European Data Protection Board 2020, nr. 130). In this case, however, it is still important to verify the age of users to ensure that children are indeed not using the adults-only service. A gratuitous statement that the service is not intended for children is therefore not sufficient and processing of personal data based on consent by a child who has not reached the age of digital consent will be unlawful.

The GDPR does not prescribe the method of age verification to be used. The choice of an age verification method depends on the risk involved in the processing of personal data (European Data Protection Board 2020; Data Protection Commission Ireland 2020). According to the EDPB, the method of age verification must be "proportionate to the nature and risks of the processing activities" (European Data Protection Board 2020, nr. 132). According to the Data Protection Commission Ireland (2020), criteria include type of personal data processed, the sensitivity of that personal data, the type of service being offered to the child, the accessibility of the personal data collected to others and the sharing of personal data with others (section 5.7.) Furthermore, one can also look at the criteria that apply to determine whether there is high risk data processing and, consequently, a DPIA (Article 35 GDPR) must be carried out. The fact that the personal data of vulnerable persons, ie. children (see Recital 38 GDPR) are processed is, besides monitoring online behaviour and profiling users, in itself a relevant factor on the basis of which a high risk character of the data processing should reasonably be assumed (Van der Hof and Lievens 2018). Note that here we focus on data processing risks, but from a children's rights perspective risk must be understood more broadly as our children's analysis in section 5.5. will show (see also (5Rights Foundation 2021; UNICEF 2021). As a result, a comprehensive analysis in the form of a combined data protection and child rights impact assessment may be required to determine the appropriate level of age verification for any digital service that impacts children.

From a data protection perspective, at low risk, a method that is not watertight will suffice, such as asking the user whether they are under or over a certain age (self-declaration). Although it is easy for the user to enter a wrong age, there are strategies to make this method more effective (5Rights Foundation 2021). Such a method is actually only suitable if the digital service performs age-appropriate data processing and no special protection of children's data protection rights is necessary. Furthermore, as a provider of a digital service, you can assume that you are indeed dealing with a child if their stated age is below 18. For high-risk data processing, a more reliable method will have to be chosen (European Data Protection Board 2020, nr. 135). Services that process personal data of minors, monitor online behaviour and profile users are likely to be engaging in high-risk processing (see Article 35; Van der Hof and Lievens 2018) and therefore need high assurance methods to verify age.

Any method that processes personal data must itself comply with the GDPR and more specifically be transparent (Articles 5 (a) and 12 et seq. GDPR) and privacy preserving (Articles 5 (c) and 25 GDPR; see section 5.4. on privacy by design). When the method is aimed at children, this means that they, and in some cases their parents, must understand how these methods use personal data in the verification process (Article 12 (1) GDPR). The principle of transparency and data minimisation go hand in hand: the more limited the data processing is, the better it is likely to be explained to children.

Age verification methods may need to be revised at regular intervals if the design of a digital service is changed in a way that has an impact on data processing (European Data Protection Board 2020, nr. 135) or because new verification methods emerge (European Data Protection Board 2020, nr. 146; Data Protection Commission Ireland 2020). Moreover, new standards for age verification are emerging (5Rights Foundation 2021).

5.4. Data protection by design

Verification of age or parental consent should not lead to excessive data processing (European Data Protection Board 2020, nr. 135, 137, 145).[6] Data processing by any kind of method must comply with the data minimization principle of Article 5 (c) GDPR which provides that personal data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. Moreover, the processing of personal data for the purpose of age verification or verification of parental consent must obviously have a lawful basis within the meaning of Article 6 GDPR in order to be lawful. Some of the lawful grounds explicitly mention the principle of necessity (e.g. contract (Article 6 (1) (b)

[6] See also D2.4. on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 28, although it was about parental controls, privacy-invasive techniques are not viewed positively by user groups.

GDPR) and legitimate interest (Article 6 (1) (f) GDPR)). In that context, the purpose limitation and specification principle is also relevant, as the lawful ground must be explicitly linked to a specific purpose for data processing and may not be processed in a way that is incompatible with that purpose (Article 5 (1) (b) GDPR).

The Audiovisual Media Services Directive explicitly states with respect to age verification and parental control systems that "personal data of minors collected or otherwise generated by video-sharing platform providers shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising" (Article 28b (3), Directive 2018/1808/EU). This is true, also, for age verification and parental consent mechanisms more generally.

Furthermore, digital service providers must implement mechanisms to demonstrate that data processing complies with the GDPR, including e.g. data minimization (i.e. the accountability principle; Article 5 (2) and 24 GDPR). In addition, pursuant to Article 25 GDPR,[7] they must implement both "appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner" (*data protection by design*) and "appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" (*data protection by default*). The principle of data protection by default is particularly relevant because children often do not change their privacy settings (Livingstone, Stoilova, and Nandagiri 2019) and it is therefore safest to set them to the most privacy-friendly default setting. This may include turning off personalised services for children by default. Data protection by design encompasses the principle of data minimization but is also broader in the sense that other data protection principles and rights can be implemented by design. This offers, among other things, opportunities for taking into account the special protection of children and their data by designing it in a child-friendly way that is transparent and accessible to them (Van der Hof and Lievens 2018; Livingstone, Stoilova, and Nandagiri 2019).

The principles of data minimization and privacy by design apply regardless of whether there is low-risk or high-risk processing that may require different forms of verification of age or parental consent (see sections 5.2.4. and 5.3.). Verification with a low degree of certainty through self-declaration can ask yes/no questions, such as are you older than ...? or are you the parent of the person that is registering for an account? Verification means that you do not need to have exact data about a person's attributes (such as age), which reduces the amount of personal data collected (Nash et al. 2013; UNICEF 2021).

[7] See also on Article 25 GDPR and the best interest of the child: Ayça Atabey, Data protection in children's best interests: what's at stake?, https://digitalfuturescommission.org.uk/blog/data-protection-in-childrens-best-interests-whats-at-stake/.

Another low assurance privacy-friendly method of estimating age is capacity testing where the child has to solve a task or puzzle that indicates their possible age (5Rights Foundation 2021). Some verification methods that provide a high degree of security, such as hard identifiers like ID cards, may involve unnecessary processing of personal data (5Rights Foundation 2021).[8] Authentication methods that use biometrics, such as facial recognition or analysis, also raise privacy issues because depending on the design of the verification process (is the person uniquely identifiable?) they may use sensitive data (Article 2 (14) and 9 (1) GDPR). Profiling children to estimate their age can also lead to excessive data processing and the creation of detailed profiles and thus does not necessarily seem to be in the best interests of the child (Van der Hof, Lievens, and Milkaite 2019; Van der Hof et al. 2020; 5Rights Foundation 2021).

Digital service providers may consider using trusted third parties (TTPs) to verify age and parental consent that offer privacy by design solutions with a high level of assurance (European Data Protection Board 2020, nr. 137).[9] This allows the digital service provider, in the spirit of the data minimisation principle, to process less personal data. Such TTPs can develop specific services based on Privacy Enhancing Technologies (PETs) which have been recommended by WP29 to be used for, among others, age verification by social networking services (Article 29 Data Protection Working Party 2009). An example of a privacy by design strategy is for the age verification provider not to process any personal data themselves because the verification process is decentralised and runs on the user's device (e.g. by using age tokens) (UNICEF 2021; 5Rights Foundation 2021). This has the advantage of not having to maintain a central database with large amounts of personal data that is vulnerable to security risks and being able to use different data sources in the verification process (Nash et al. 2013; UNICEF 2021; 5Rights Foundation 2021). Furthermore, the provision of open source age verification can contribute to the transparency and security of such methods. An example of a verification service that is both decentralised and open source is IRMA offered by the Privacy by Design Foundation.[10]

Another example of a privacy by design strategy is for the verification process to be completely anonymized (although this is not easily achieved, AEPD and EDPB 2021). In that case, there is no personal data processed and the GDPR does not apply. In the case of pseudonymisation (see section 3), however, personal data is still processed and the GDPR applies, but it is still an important privacy by design strategy (Article 25 GDPR). Or personal

[8] See also D2.4. on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 25-26.
[9] See also D2.4. on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 25-26, but also pointing out that these may be expensive solutions for digital service providers.
[10] See https://irma.app/?lang=en. See also D2.2 EU Methods for AVMSD and GDPR Compliance Report for an overview of age verification methods.

data is deleted as soon as the verification session is completed but then the GDPR will still have to be complied with because personal data is processed and the digital service provider must be able to show that age and parental consent have been verified in a reasonable manner (given the risk involved) (see also Article 5 (2) GDPR). More generally, the initial design of consent and age verification systems can benefit from these and other privacy design strategies as presented by Hoepman (2020) to help make fundamental privacy design choices.

5.5. Consent and age verification from a children's rights perspective

5.5.1. Introduction

The Committee on the Rights of the Child recognised in General comment No. 25 (2021) on children's rights in relation to the digital environment that children have a fundamental right to data protection based on Article 16 CRC (Committee on the Rights of the Child 2021). Thus, the UN Convention on the Rights of the Child has become directly relevant to protecting children when their data is processed by digital service providers. At the same time, through the best interests of the child principle, the Convention already applies to any activity that has an impact on children, including the activities of digital service providers when children use them. This section will therefore explain how the Convention on the Rights of the Child applies to data protection and, in particular, to age verification and consent mechanisms. Section 5.5.2. will address the general principles of the CRC. Section 5.5.3. will provide an analysis from the perspective of the three types of, partly overlapping, children's rights recognized by the CRC, i.e. protection, participation and provision rights (Alderson 2008).

5.5.2. General principles

The UN Convention on the Rights of the Child has four fundamental principles that must be used in the interpretation and implementation of children's rights. These general principles are the principle of non-discrimination (Article 2 CRC), the best interest of the child (Article 3 CRC), the right to life and development (Article 6 CRC) and the right to be heard (Article 12). In the next sections, each of these principles will be briefly elaborated in relation to data protection, consent and verification methods.

5.5.2.1. Non-discrimination

The principle of non-discrimination means that the rights of the child apply equally to all children, albeit the implementation of rights may be different given e.g. the best interest (Article 3 CRC) or the evolving capacities of the child (Article 5 CRC). Children have a fundamental right to data protection and it should therefore not be context-dependent whether that protection is actually guaranteed in a legal or practical sense. Furthermore, children should not be banned from digital services without a legitimate reason. The fact that certain services are unsuitable or even harmful for children can be a legitimate reason not to give them access. However, in the context of the evolving capacities of children (Article 5 CRC), their age must be taken into account: what is unsuitable for younger children is not necessarily so for older children, such as adolescents. Generally, the right to non-discrimination entails that children have equal effective and meaningful access to digital services and digital exclusion of children must be prevented (Committee on the Rights of the Child 2021).

The principle of non-discrimination is also relevant in the design and implementation of verification methods and consent mechanisms. Any method chosen for age verification or parental verification must not discriminate against particular groups of children, e.g. by excluding them. For example, the EDPB states in its opinion that if a bank or credit card transfer is used to verify parental consent (see section 5.3.1.) then an alternative method must be available for parents who do not have a credit card or bank account (European Data Protection Board 2020, fn 68). The same is true when a child, or their parent for that matter, does not have access to an (e)ID card (UNICEF 2021). Similarly, methods for parental verification must also be available for children whose parents may not be present to consent on their behalf, such as in the case of refugee children staying in another country than their parents or children that are placed in care (UNICEF 2021). In that case, someone other than the parent and possibly the guardian must be able to give consent.

Moreover, the development of verification methods should also avoid the use of technologies that are potentially biased towards certain groups of children and/or their parents, unjustifiably exclude them or give a high probability of false results, e.g. by not working well with specific personal characteristics, such as skin tones, ethnicities, gender, disabilities or age (5Rights Foundation 2021; UNICEF 2021). It should also be taken into account that verification methods covered by Article 22 GDPR (on automated decision making and profiling) may not be allowed with regard to children due to the very restrictive interpretation of the exception to the prohibition of automated decision making in that case. The bottom line is that automated decision making is presumably only allowed if it is in the best interest of the child (Van der Hof, Lievens, and Milkaite 2019; Van der Hof et al. 2020). A

system that uses a more privacy invasive method than is necessary and may have a discriminatory effect is not in the best interest of the child.

5.5.2.2. Best interest of the child

The obligation to take the best interests of the child as a primary consideration in all activities that have an impact on children can be found in Article 3(1) of the UN Convention on the Rights of the Child, 1989 and Article 24(2) of the Charter of Fundamental Rights of the European Union. The implementation of the best interests of the child requires a concretisation of all relevant children's rights when designing a digital service with an impact on children. Relevant children's rights may include: the right to freedom of information, expression and thought (Article 13 and 14 CRC), the right to freedom of association (Article 15 CRC), the right to privacy and data protection (Article 16 CRC), the right to access (non-harmful) media (Article 17 CRC), the right to protection against violence (including bullying and sexual abuse) (Article 19 and 34 CRC) the right to play and recreation (Article 31 CRC), and the right to protection against against economic exploitation (Article 32 CRC). The best interests of the child are therefore not only about preventing harmful activities for children but also about contributing to the well-being of children in a broader sense. Moreover, the best interest of the child is inextricably linked to the right of the child to be heard (Article 12 CRC), because in order to find out what is in the best interest of the child, you also have to involve the views of children themselves (Committee on the Rights of the Child 2013).

When implementing relevant children's rights, a balance must be struck between children's data protection rights and their other rights, including their rights to development (Article 6 CRC), freedom of expression and information (Article 13 CRC) and association (Article 15 CRC). In addition, the age of children and their evolving capacities must be taken into account (Article 5 CRC). Some design choices may be in the interest of a 16-year-old but not in the interest of a 6-year-old. With younger children, it may be justified to place greater emphasis on their protection rights, while with older children, freedom rights become more important (UNICEF 2021; see also sections 5.5.3.1. and 5.5.3.2.). Also requiring children to be represented by their parents or another adult when consenting to the processing of their personal data can be seen as being in the best interest of the child, when a child is unable to do so on its own (Council of Europe 2018; UNICEF 2021). At the same time, parental consent can also be contrary to the interests of the child in, for example, sensitive situations that the child does not want to share with the parents. For this very reason, counselling services are excluded from Article 8 GDPR (Recital 38 GDPR). Special attention should be paid to making digital services (including age verification and parental consent mechanisms) accessible to children who face specific challenges such as physical and intellectual disabilities or difficult private situations in which adequate parental or other guidance may not always be present.

The latter is particularly relevant when parental consent is required to lawfully process personal data.

The WP29 has emphasised the importance of implementing the best interest of the child principle (Article 3 CRC) with regard to the processing of children's personal data in the school and educational environment as well as in relation to social media (Article 29 Data Protection Working Party 2008, 2009). The GDPR aims, inter alia, at contributing to the 'well-being of natural persons' (Recital 2). However, the best interest of the child is most clearly expressed in Recital 38, which states that children enjoy specific protection in the light of their fundamental right to data protection. Other Recitals in the GDPR also emphasise the specific protection of children: Recital 58 (transparency of data processing), Recital 65 (right to be forgotten), Recital 71 (automated decision-making and profiling), Recital 75 (processing of personal data of children is risky). These Recitals are to a certain extent regulated in the provisions of the GDPR.

Irrespective of the application of Article 8 GDPR more specifically, in order to apply the GDPR in the interest of the child in practice, it is necessary to know if and when you are dealing with children, i.e. persons under 18. This can be done through age verification, after which the special protection of their personal data can be specifically taken into account with underage users of a service. In particular, this may imply that the extent to which children have reached the age of digital consent when Article 8 GDPR applies should also be considered. But as mentioned earlier, the protection of children under the GDPR goes beyond mandating parental consent for some age groups. Moreover, in order to determine the impact of an activity on children and their rights, in this case the use of digital services, age verification methods and parental consent mechanisms, it is necessary to carry out a children's rights impact assessment (Committee on the Rights of the Child 2013; UNICEF/Danish Institute for Human Rights 2013; 5Rights Foundation 2021; Mukherjee, Pothong, Livingstone 2021). This should prevent that only GDPR compliance is leading in the design and development of parental consent and age verification methods and ensure that the rights of children are also taken into account (UNICEF 2021).

5.5.2.3. Right to life and development

The child’s right to life and development (Article 6 CRC) contains an obligation for states to ensure, among others, children’s optimal development. Development must according to the CRC Committee be interpreted “its broadest sense as a holistic concept, embracing the child’s physical, mental, spiritual, moral, psychological and social development” (Committee on the Rights of the Child 2003). In the EU, the right to development may be connected to the right to informational self-determination and, more

specifically, the right to control over personal information and the rights to privacy and data protection (Van der Hof 2017).

Obviously, the child's evolving capacities (Article 5 CRC) are important when it comes to the question of whether children are capable of exercising their right to informational self-determination themselves or whether they need the help of an adult to do so. This is also the underlying consideration for Article 8 GDPR parental consent, as only from a certain age can children themselves consent to the processing of their personal data. The question whether children are actually capable of doing so also depends on the individual development of the child, the complexity of the data processing and the age-appropriate nature of the information provided about the data processing (see also on a child's capability to exercise their data protection rights: Data Protection Commission Ireland 2020). Although Article 8 GDPR leaves room to take evolving capacities into account, we have no evidence that the determination of the ages for digital consent in that provision or the national implementations in the EU Member States is evidence-based.

It is worth recalling here that consent covers only a small part of data processing and therefore a child-centred interpretation of the other provisions of the GDPR is required in order to effectively guarantee their fundamental right to data protection (Van der Hof, Lievens, and Milkaite 2019; Van der Hof and Lievens 2018; Committee on the Rights of the Child 2021). More generally, it should be borne in mind that digital services can make a hugely important contribution to children's development and should therefore be accessible to children. At the same time, providers must ensure that their digital services do not have a harmful impact on children. The design of the technologies will therefore have to take into account the realisation of a positive contribution to children's development and the prevention of harmful effects on them (Committee on the Rights of the Child 2021).

5.5.2.4. Right to be heard

The right to be heard (Article 12 CRC) provides that "States parties shall assure to the child who is capable of forming his or her own views, the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child." The right to be heard is inextricably linked to the best interest of the child (Article 3 CRC) (Committee on the Rights of the Child 2009, 2013). As the Committee of the Rights of the Child (2013) says: " The two articles have complementary roles: the first aims to realize the child's best interests, and the second provides the methodology for hearing the views of the child or children and their inclusion in all matters affecting the child, including the assessment of his or her best interests". In other words, whenever the best interests of the child have to be established with regard to their data processing, children must be heard, although in practice this often still does not happen

(Lievens, Livingstone, Mc Laughlin, et al. 2018). In relation to this the Irish Data Protection Commission considers the exercise of their rights by children, such as their data protection rights, to be closely related to the expression by the child of its views (Data Protection Commission Ireland 2020).

As a result, children will need to be involved in some way in the design and development of verification and consent mechanisms as these impact on their use of digital services. Particularly, children must be consulted on the age appropriate nature of digital services and any age gating for the purposes of their protection (UNICEF 2021). Moreover, the choices made in the design process of verification and consent mechanisms may have an impact on their (other) rights, including their best interests, which makes involving children important as well.

5.5.3. Protection, participation and provision

5.5.3.1. Protection rights

When it comes to the protection of rights of children, the right to data protection is central to this study. The Committee on the Rights of the Child indicates that the CRC, and in particular Article 16 on the right to privacy, contains a right for children to data protection. Moreover, EU citizens, including children, have a fundamental right to data protection pursuant to Article 8 (1) Charter of Fundamental Rights of the European Union (EU Charter) and Article 16 (1) Treaty on the Functioning of the European Union. The fundamental right to data protection is elaborated in, among others, the GDPR which states that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right" (Recital 1 GDPR). Moreover, Recital 4 GDPR provides that the GDPR "respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity." "All fundamental rights" includes the rights of children and in particular the best interests of the child (Article 3 CRC, Article 24 EU Charter) (see section 5.5.2.2.) and the right of children to be heard (Article 12 CRC) (see section 5.5.2.4.).

The special protection that the GDPR aims to give to children and their personal data applies in principle to all children regardless of their age. This means that even when children have reached the age of digital consent and can therefore decide for themselves about the processing of their personal data, the digital service provider will still have to take into account their status as children (Recital 38 GDPR; Van der Hof, Lievens, and Milkaite

2019). Circumventing the rules of the GDPR by - effectively or not - excluding children under a certain age, by what is called age gating, and not providing significant age-appropriate protection to other children does not do justice to children's data protection and other rights (Data Protection Commission Ireland 2020; UNICEF 2021).

Moreover, the right of children to data protection as a protection right includes the obligation for data controllers to ask parents to give consent to the processing of personal data of their children when children themselves are not able to understand how their personal data is processed and what the possible risks are (Recital 38 GDPR). In order to use consent as a mechanism to enable parents or children to *effectively* protect personal data by controlling its use, data processing should be understandable and therefore not too complicated (informed consent), and the choice to consent to data processing should be free (free consent), unambiguous (an affirmative action), and can easily be withdrawn (Article 7 GDPR) (Committee on the Rights of the Child 2021). Adequate data protection also means that verification and consent mechanisms themselves process only necessary personal data (Article 5 (c) GDPR) and also otherwise demonstrably comply with the provisions of the GDPR (Article 5 (2) GDPR), which in the case of children means that their best interests are taken into account (Van der Hof, Lievens, and Milkaite 2019; ICO 2020; Data Protection Commission Ireland 2020).

Furthermore, consent, and in our case parental consent, aims to legitimise an act by the data controller that would otherwise infringe the right to privacy and data protection (Schermer, Custers, and van der Hof 2014) and is therefore not intended as a tool for parental control or parental surveillance of children's behaviour. Nevertheless, parental consent can be used by parents for the latter purposes, because to a certain extent they gain insight into their children's online activities whenever they must consent to them signing up to a digital service. As a result, consent mechanisms can have an impact on children's right to privacy from their parents (Lievens, Livingstone, Mc Laughlin, et al. 2018).[11] This is especially problematic if children want access to, for example, services or information that they are not (yet) happy to share with their parents, such as dating services and gender related or sexual information. Although younger children also have a sense of privacy in relation to others, including their parents, this problem becomes more pressing the older children get (Van der Hof 2017). Since the ages for digital consent are legally established by the EU Member States, it will be difficult to take this into account when designing consent mechanisms, especially as parents should be able to assess data processing determined by the controller before agreeing. However, for the purpose of providing parental consent, the parent's access may be limited to gaining insight into the data processing envisaged by the provider, without

[11] See also D2.4. on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 28, although this applied to parental controls, more specifically, measures that are considered too restrictive or invasive by children can lead to a decrease in trust between parent and child.

further revealing how the account is used. As a matter of fact, the child's right to privacy can in this case be regarded as both a protection right (for example not sharing personal and sometimes intimate information) as well as a right of participation (for example the right to develop a sexual identity through the intimate interaction with peers). Although we distinguish between the different types of rights here, specific children's rights can fall into different categories.

Given the fact that consent is a legal act to legitimise specific data processing activities by the data controller that would otherwise infringe the right to privacy and data protection, and, therefore, not a parental control tool, we will not focus in this study on other protection rights in relation to children's use digital services, such as their rights to protection from harmful content (Article 17 (e) CRC), to protection from violence (Article 19 CRC), and to protection from economic exploitation (Article 32 CRC). Having said that, it is of course important that parents, as the primary responsibility for their children (Article 18 CRC), consider the best interests of their child (Article 3 CRC) as well as their evolving capacities (Article 5 CRC) when deciding whether to give them access to digital services, including the processing of personal data by those services. In addition, providers of digital services - regardless of whether consent is the lawful basis for data processing - will also have to take into account the best interests of the child - including a precautionary approach to potentially harmful effects - when designing and developing their services. Verification methods are therefore a broader obligation than just under Article 8 GDPR which is central to this study.

5.5.3.2. Participation rights

Participation means that "individuals and groups of individuals having the right, the means, the space, the opportunity and, where necessary, the support to freely express their views, to be heard and to contribute to decision making on matters affecting them, their views being given due weight in accordance with their age and maturity" (Council of Europe 2012). Typical participation rights thus clearly are the right to be heard (Article 12 CRC), the right to freedom of expression (Article 13 CRC) and the freedom of association (Article 15 CRC).

When it comes to children's right to be heard, it is relevant to include children's wishes, needs and views when developing and implementing age verification and parental consent mechanisms. This could be user testing of such methods, of course, but also more specifically the views of children on the impact on their rights, such as their right to privacy or freedom of information, when these methods are implemented. By involving children, you can better connect to their experiences and gain insight into what obstacles they experience

when using or being subject to such methods. In any case, this makes hearing children an important part of carrying out a children's rights impact assessment (see section 5.5.2.2.).

Being able to consent to the processing of personal data oneself is also a form of participation that is of course subject to the age of digital consent set out in Article 8 GDPR. In this respect, it is interesting that France has chosen to rely on joint consent when a child has not yet reached the age of digital consent. In that case, the child must also give consent in addition to the parent (see section 5.2.3.).

Under the GDPR, age verification and parental consent mechanisms are primarily intended to protect children from unlawful or inappropriate processing of their personal data when they are not yet able to make independent decisions about the processing of their personal data or are particularly vulnerable with regard to the processing of personal data. However, there is also a participation dimension to this in several ways. In practice, extra protection for children leads to their exclusion from digital services. Of course, companies have the freedom to do business (Article 16 EU Charter of Fundamental Rights) and are also free to decide for themselves with whom they conclude contracts (freedom of contract) (Silva 2021), but if the exclusion of children is only intended to circumvent the law, in this case the GDPR, then the situation is different. In that case, apparently companies do want to admit children as users (after all, they are interesting customers) but do not seem to want to take their specific rights and interests into account (see also Data Protection Commission Ireland 2020; 5Rights Foundation 2021). This situation exists because easily circumvented age verification methods are used (see chapter 3).

The question is, however, what happens if age verification is taken seriously and stricter methods are designed and implemented that can effectively exclude children from platforms. Will their protection rights be taken into account so that they can continue to use digital services, or will they be excluded because it is too complicated or expensive to develop truly child-friendly digital services? And might it also become more difficult for startups to compete with established tech companies that have the resources to offer adequate age verification and age appropriate services? It seems that the larger digital service providers are investing in age verification systems (UNICEF 2021). In any case, children should not be deprived of a rich user experience or be offered inferior digital services purely on the basis of alleged data protection considerations. Rather, digital service providers should provide age-appropriate privacy-by-design services that respect children's rights (Data Protection Commission Ireland 2020).

Furthermore, parental consent can also have an impact on children's participation rights, especially their rights to privacy, freedom of information and expression. The legal requirement to ask parents (or other adults) for consent to process personal data may be

perceived by children as a barrier to using digital services freely, i.e. out of sight of parents (Van der Hof 2017). Social media can by teens, for instance, be perceived as spaces that allow them to escape from their parents or at least to meet and communicate with their peers (boyd 2008). For children privacy means privacy from parents (Shmueli and Blecher-Prigat 2011). Some quotes from a study among 213 Dutch children aged 11-16 years, clearly show the privacy sentiments that are raised by the parental consent requirement: "If I have to get permission from my parents, I'm going to lie that I'm 16 years old, because it harms my privacy!" (an 11 year old boy), "Teach, are you kidding? 16 years old? What kind of lawmaker is that? Don't they understand we really need our privacy?!" (a 14 year old student), "If you have to ask your parents for permission in every case, you don't have a private life anymore" (an 11 year old girl), "My private life will be harmed, because I would have to ask everything to my parents, and will not have the possibility to explore and search for myself" (an 11 year old boy) (Kwantes 2017). Moreover, children also consider guidance by parents to be important, and involving parents in giving parental consent can contribute to this (Kwantes 2017). Of course, such privacy tensions only arise if parental consent is required, which is when consent is the appropriate lawful ground (see section 5.2.1.). Moreover, when designing parental consent mechanisms, these sensitivities can be taken into account by only giving parents access to information about the specific data processing for which consent is requested.

5.5.3.3. Provision rights

Provision rights focus on, among others, the access of children to resources and services. The right to education (Articles 28 and 29 CRC) is for instance a typical provision right. From a data protection perspective, investing in data literacy is important so that children who have reached the age of digital consent can make good decisions with regard to the processing of their personal data by deciding whether or not to give consent. To what extent they are actually able to do so, especially given the complexity of data processing, is open to question (Stoilova, Nandagiri, and Livingstone 2021), although consent is only informed (and therefore potentially lawful) if children understand how personal data is processed. Moreover, even before children have reached the age of digital consent, it is important that they gain insight into the how and why as well as the possible risks of data processing. Firstly, because the law sometimes requires that the data processing is jointly consented to by the parent and the child (i.e. in France, see section 5.2.3.). Second, as part of the development of the child who at some point reaches the age of digital consent and therefore needs to understand how tech companies use data. Furthermore, data literacy is also relevant for enabling children to exercise their data subject rights. In the context of the design of digital services, the right to be heard is instrumental here (see section 5.5.2.4.), as is the transparency principle (Article 5 (a) GDPR) which requires specific attention in relation to children (Article 12 (1) GDPR) (Milkaite and Lievens 2020). It also means that providers of

digital services must deploy resources to design their services, including the associated verification and consent mechanisms, in a child-friendly and age appropriate manner (see (ICO 2020; Data Protection Commission Ireland 2020).

In addition, the design of digital services that process data from children must also provide opportunities in a way accessible to children and parents to be able to exercise data subject rights in the GDPR quickly and effectively. In the context of this study, the ability to easily withdraw consent must be part of consent mechanisms (Article 7 (3) GDPR). Incidentally, the GDPR is not entirely clear here because Article 8 indicates when parents must give consent but there is no comparable provision when it comes to withdrawing consent. It seems logical that the person giving consent is also authorised to withdraw it. At the same time, children could also simply switch off consent for personalized advertising, for example, since less data would then need to be processed. Only when they turn the option back on would the parent have to give consent separately. Children should also be made aware of the possibility to withdraw consent - in a way understandable and accessible to them - when they reach the age of digital consent themselves, as they may wish to review data processing operations for which parental consent has been given. In addition to withdrawing consent, within the settings of the service, parents and children must be given the possibility to object to data processing in a simple manner. Even if consent is not required as a lawful basis, it may be that parents and children do not consent to the data processing and can object on good grounds, such as when the provider of a digital service cannot demonstrate having an overriding legitimate interest (Article 21 (1) GDPR) or in the case of processing for direct marketing purposes (Article 21 (3) GDPR).

Finally, the (protection and participation) rights of children must be protected by providing them with access to effective and child friendly instruments to enable them to make complaints when their rights are not observed or get support in using such instruments (Council of Europe 2012; Lievens, Livingstone, McLaughlin, et al. 2018). It is important that children can, for example, complain to their data protection authority (Article 57 (f) GDPR) if they feel that their data protection rights are not sufficiently respected, either by themselves or through a legal representative (Data Protection Commission Ireland 2020). Digital service providers, including age verification providers, are also advised to provide easy to use, age appropriate online tools to exercise data protection rights, such as children's access rights, or to lodge a complaint (ICO 2020).

6. Consent mechanisms in apps and games

6.1. Introduction

This chapter provides an overview, analysis and assessment of age verification and consent mechanisms in apps/games popular among children and likely to be used by children, and particularly focuses on the ways in which they factor in legal requirements for such mechanisms as identified in the previous chapter.

First an analytical framework is developed (section 6.2.) which will then be applied to map age verification and parental consent methods in apps and games that have been identified as popular among or likely to be used by children (for mapping results, see Annex1). Section 6.3. provides an analysis of the age verification and parental consent mechanisms identified in the apps and games. Section 6.4. assesses both these methods from the perspective of data protection and children's rights.

6.2. Selection of apps/games/platforms and Analytical framework

This section maps parental consent mechanisms in selected apps and games (likely to be) used by children. A selection has been made of apps, games and platforms[12] that are popular with children. The popularity is based as much as possible on evidence (see Technical report in Annex 1) but also on best guess choices because data is not always available. The selection of apps is as follows:

- Discord
- Facebook
- Instagram
- Pinterest
- Snapchat
- Tiktok
- Twitch
- Twitter
- YouTube
- Yubo (and Yoti)

[12] Websites may also be included, e.g. because some digital services can be accessed both through apps and websites, or because the sign-up process is accessible through a website.

Although some are more associated with children or teenagers, such as TikTok, Instagram, Youtube, and Snapchat, all of these apps are well-known or popular services that are also used by children.

The selection of games[13] is as follows:

- Among Us
- Call of Duty
- Clash of Clans
- FIFA
- Fortnite
- Grand Theft Auto
- League of Legends
- Roblox

Moreover, we have analysed the following platforms:

- Apple
- Google
- Microsoft
- Nintendo
- Playstation
- Steam

Only apps/games/platforms where consent is used as one of the lawful grounds for data processing have been included in the study. As a result, apps that initially fell within the selection, such as Only Fans, were dropped after the initial analysis. The technical analysis was for the greatest part carried out in the period April - May 2021 and we only made adjustments whenever we found new or additional information after starting to write the overview (Section 6.3.) and assessment (Section 6.4.).

The apps and games are reviewed based on factors arising from the analysis of consent by children and parents under the GDPR. This results in the following factors:

- Is consent used as a lawful ground for data processing?

[13] The best-selling video game Minecraft (a game for PC, mobile and several console platforms) released by Mojang Studios was not included in this technical analysis. Mojang studios is owned by Microsoft and Microsoft's Privacy Statement and Terms of Use are applicable. Therefore there is no added value to discuss Minecraft in a separate section. Microsoft is discussed in Section 3.3. of the Technical Report (Annex 1).

Only if consent is used as a lawful ground will parental consent be required when personal data is processed of a child under the age of digital consent.

- What age verification method is used?

In order to establish whether a user is under the age of digital consent the age of users must be verified. The method of age verification must be "proportionate to the nature and risks of the processing activities". High risk data processing, such as processing children's personal data and profiling of users, are likely to require methods that provide more age assurance than a self-declaration by users.

- What personal data is used for age verification?

In connection with the principles of data minimisation, data protection by design and data protection by default, the implementation of age verification should avoid processing more personal data than is necessary to adequately carry it out given the context (e.g. low risk vs high risk data processing).

- How is parental consent obtained?

If the child has not yet reached the age of digital consent, the parent or someone else who has responsibility for the child must give consent on their behalf.

- How is parental consent verified?

In order to establish that it is indeed the parent who gives consent, some verification of their position as a parent will have to take place.

- How is it possible for legal representatives of the child, other than the parent, to give consent?

If a parent as the holder of parental authority is not available, someone else who has responsibility for the child must also have the opportunity to consent on the behalf of the child, and some verification of their position as a holder of parental authority (or guardianship) will have to take place.

- Is there joint consent and how is it obtained?

In some Member States, joint consent of parent and child is necessary if the child has not yet reached the age of digital consent.

- What personal data is used for obtaining verifiable parental consent?

In connection with the principles of data minimisation, data protection by design and data protection by default, the implementation of verification of parental consent should avoid processing more personal data than is necessary to adequately carry it out given the context (e.g. low risk vs high risk data processing).

In order to gather data for the substantiation of the various factors, research will be carried out into the privacy policies of the apps and games, the method of signing up and the account settings that users can adjust. Prior to each analysis, a short description of each app and game is given (see Annex 1 for the results).

The purpose of the analysis of a selection of apps and games that are (potentially) used by children is to gain insight into the age verification and parental consent methods used and to identify good practices from the perspective of compliance with Article 8 GDPR.

6.3. Overview and analysis of age verification and consent methods

This section will provide an overview of the results of the study of the selected apps/games/platforms based on the analytical framework in Section 6.2 (see Annex 1 for full results). First we will discuss age verification and then parental consent methods.

6.3.1. Age verification[14]

The analysis of the apps and games shows that the most commonly used method is self-declaration, as the user has to enter a date of birth when registering for the service in question. This is the case with Discord, Facebook, Instagram, Snapchat, TikTok, Twitter, Among Us, Call of Duty: Modern Warfare, FIFA, Grand Theft Auto, League of Legends, Roblox, Apple ID, Google (including Youtube), Microsoft (including XBox), Nintendo and Steam. Pinterest asks users to provide their age instead of a date of birth. These are all clearly methods with a low level of assurance. Children can easily enter a date of birth other than their own if, for example, the app or game excludes children under a certain age (e.g.

[14] In some cases, you can also sign on to an app or game using an account from another digital service, such as Facebook, Google or Steam. In these cases, however, we have always chosen to use an email address to log in instead of signing on with a third-party account.

under 13) from accessing the service.[15] If the app or game is child-friendly and privacy-friendly by default, such a method may be sufficient. However, as many of these apps and games are not specifically designed for children, we assume that a higher level of certainty with regard to age verification is necessary. In the case of the Apple ID, parents can create an ID for their children under 13. The age is verified on the basis of the self-declaration of a date of birth of the child. The same is true for a Google or Microsoft family account. Nintendo has added a second verification by asking users whether they are aged 15 or under or aged 16 or over. In the first case a child account must be created that will be added to a parental account. The accounts are still created by the self-declaration of a date of birth (for parent and child respectively), though the child's date of birth can not be changed later.

Some apps use a different form of age verification besides self-declaration. For instance, Yubo asks for a date of birth and a photo which will be age estimated with face geometry technology. In case of reasonable doubt about the reported age, the account must be verified, and the user is required to send a screenshot of their ID or school card, and record a short video in which they pronounce three random words. Age estimation is provided by the third party age verification service provider Yoti. If a user objects to age estimation in their settings (hence, interestingly, this is opt out rather opt in) or you cannot use Yoti,[16] the age of the user is verified through 3 photos, i.e. a photo of one of the supported IDs[17] (if the school card, grade and school year are fully visible), a photo of the user holding their ID next to their face, and a photo of the user holding a 'Yubo Team' sign and today's date (in the latter two cases the face must be fully visible). If the user uses Yoti for age verification, they first need to create an account after downloading the app. Yoti requires the user to provide a phone number, face scan, and an ID card (passport, driving license or national ID) showing birth date if the app is used for age verification in Yubo. You can only use Yoti if you have reached the age of digital consent, as you must consent to the use of what Yoti calls 'biometric data' (i.e. a face scan). Since it is necessary to show an ID with date of birth when you use Yubo's or Yoti's[18] age verification method it is a bit strange

[15] See also D2.4. on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 26, pointing out that parents help children to circumvent age restrictions.
[16] This may be the case when the user doesn't have a Yoti supported ID, is too young to use Yoti (which is when the child is under the age of consent given that you have to explicitly consent for the use of biometric data by Yoti) or Yoti is not available in their country.
[17] Supported IDs are "Driver's License, State ID, Passport, National ID, Military ID, School ID card (if we can see your birthdate or if your grade and school year are visible - We also cannot accept School IDs from students in grade 7 or 12), Medical card (the document needs to contain your full name, a picture of you as well as your birth date), Green card, Young Scot card, Temporary residence card" Yubo also accepts Birth Certificates, but this needs to be supported with any other ID that shows the full name and a recent photo of the user (e.g. library card, bus pass, swimming pool card, etc) to enable cross-reference the details to the birth certificate", https://support.yubo.live/hc/en-us/Articles/360010700259-Accepted-IDs (accessed April 2021).
[18] Adding ID to Yoti is optional but to use this verification method in Yubo, it must be added.

that age estimation also needs to be done, because the age of the child is then already known. What is also not clear is what happens if you do not verify your age (though Yubo talks about identity, which is broader). You don't get a yellow 'verified' badge on your profile but we could still use the app.

Some services indicate that they can ask for proof of age. This is the case with TikTok although they do not say when this will happen and how the age can then be proved. This also seems to be the case with Google. If Google learns that you may not be old enough to have a Google account, you have 14 days to either set up supervision for your account or verify that you are old enough to manage your account (which you can do by providing a valid government-issued valid ID or a credit card). However, it is unclear how Google learns that a user may not be old enough to have a Google account.

When the user wants to change their age, some apps and games ask for additional information for the purpose of age verification. A user may want to change the age if, for example, it is entered incorrectly or if after entering the age the user notices that they are not allowed to access the service because they are too young (e.g. the service only allows users aged 13 and over). In the latter case, the user may be locked out and unable to create a new account immediately. Discord, for instance, requires the user to email (from their address associated with the Discord account) an ID showing a photo and birth date and their Discord tag. However, it was also easy to create a new account with a different age on another device, making this easy to circumvent. In the case of Call of Duty: Modern Warfare, Grand Theft Auto and League of Legends, Fifa, it wasn't possible to sign up with a different age in the same browser after not meeting the minimum age requirements. However, when using another browser or after deleting cookies, it was still possible to sign up with another age. In other cases, however, the user can immediately specify a different age and gain access to the service. This is the case with Facebook, Instagram, Pinterest, Snapchat, Twitch, and Twitter.

Some services have the option of reporting children who are younger than allowed to use an app or game. Children who use a wrong date of birth to access the service can then be removed by the company concerned. This is the case with Facebook where it seems that anyone can report children under 13 and if the child's age is "reasonably verifiable as under 13 years", Facebook will delete the account. How the age is verified is not clear. Instagram uses a similar procedure to report children under 13. In this case, however, it seems that the user may be asked to verify age by uploading an ID containing name, photo and date of birth.[19] Any other personal information on the ID, such as ID or social security number, may

[19] Proof of ID is categorised in two groups. You can send Instagram one of the items from group one to confirm your identity. Anything that you send Instagram should contain either your full name and photo or your full

be covered (physically, not digitally). Twitch and Discord also allow users under the age of 13 to be reported and their personal information (and likely, though not mentioned, also their accounts) will then be removed. In neither case is it clear whether and, if so, how age will be verified. Among Us has an email address where accounts of children under 13 can be reported and personal information will then be deleted.

In the case of Clash of Clans there is no age verification, not even a self-declaration, as far as we could see. However, the game can also be played through e.g. the Game Center in which case it is linked to the Apple ID (see above). Also, Fortnite does not ask their users to provide age or a date of birth, although if they want to become a creator (i.e. active video makers, streamers, storytellers, artists, cosplayers, musicians, and community builders that can earn money by creating content for Fortnite, Rocket League, and other games in the Epic Games Store) they must declare to be over 18 or if between 13 and 18 that the parent or guardian is signing up on behalf of them. Other services, namely Twitch, Youtube, and Among Us, do not necessarily require an account to be created in order to use them. In that case, there is also no age verification although personal data of children may still be processed.

In some cases, age verification is also used for purposes other than registration with the service. For example, the date of birth is used by Twitter to determine whether a user meets the minimum age requirement for certain advertising content (e.g. alcohol advertising). With Youtube some content is age restricted and requires confirmation of date of birth using a credit card or ID photo.

In the following table some of the findings concerning age verification in the apps/games/platforms are summarised[20]:

---

name and indicate your age. Items in group one include the following documents: Birth Certificate, Driver's license, Passport, Marriage certificate, Official name change paperwork, Personal or vehicle insurance card, Non-driver's government ID (example: disability, SNAP or national ID card), Green card, residence permit or immigration papers, Tribal identification or status card, Voter ID card, Family certificate, Visa, National age card, Immigration registration card, and Tax identification card.

If you don't have any of the group one documents showing a photo, you can send two different items from either group one or group two. Items in group two include the following documents: Bank statement, Transit card, Check, Credit card, Employment verification, Library card, Mail, Magazine subscription stub, Medical record, Membership ID (example: a pension card, union membership, work ID, professional ID), Paycheck stub, Permit, School ID card, School record, Social Security card, Utility bill, Yearbook photo (actual scan or photograph of the page in your yearbook), Company loyalty card, Contract, Family registry, Diploma, Religious documents, Certificate of registration for accreditation or professional, Professional license card, Polling card, Health insurance, Address proof card, and Social welfare card. Any of these documents must include full name and at least one of the documents should contain a photo and indication of age. The names on both documents must match each other.

[20] For the complete results of the performed case study research please see the Technical report in Annex 1.

Apps / Games / Platforms	Minimum Age to use the Service	Age Verification present at account creation?[21]	Type of Age Verification at account creation	Data used for Age Verification
Discord	13 “and the minimum age of digital consent in your country”.	Yes	Self-declaration	Date of Birth
Facebook	You can not use Facebook if you are under 13 (in Spain 14) years old.	Yes	Self-declaration	Date of Birth
Instagram	You must be at least 13 years old to use the service (in Spain 14).	Yes	Self-declaration	Date of Birth
Pinterest	13 and in the EEA over the age at which you can provide consent to data processing under the laws of your country.	Yes	Self-declaration	Age
Snapchat	No one under 13 is allowed to create an account or use the service.	Yes	Self-declaration	Date of Birth
TikTok	The Services and the Platform are only for people 13 years old and over.	Yes	Self-declaration	Date of Birth
Twitch	The Twitch Services are not available to persons under the age of 13. If you are between the ages of 13 and the age of legal majority in your jurisdiction of residence, you may only use the Twitch Services	Yes	Self-declaration	Date of Birth

[21] Age verification needed for account creation: This does not necessarily mean that you can not use the service without age verification. Some services can be used without an account (such as YouTube and Twitch). Age can also be verified after the account creation, in which cases often more data is requested. This is described in more detail in the Technical Report (Annex 1).

	under the supervision of a parent or legal guardian who agrees to be bound by the Terms of Service.			
Twitter	You must be at least 13 years old to use the Services	Yes	Self-declaration	Date of Birth
YouTube	You may use the Service if you are at least 13 years old; however, children of all ages may use the Service and YouTube Kids (where available) if enabled by a parent or legal guardian.	See Google	See Google	See Google
YouTube Kids	You may use the Service if you are at least 13 years old; however, children of all ages may use the Service and YouTube Kids (where available) if enabled by a parent or legal guardian.	Yes	Self-declaration	Year of Birth
Yubo	If you are under age 13, you are not permitted to use the YUBO App. If you are between 13 and 17 years old, you are not allowed to create a user profile without the permission of your legal representative.	Yes	Self-declaration + Age Estimation (via Face Geometry)	Date of Birth + Picture (for a face geometry scan)
Among Us	Age is not mentioned in the Terms of Use. The Privacy Policy states that if you are under the age of 13, you may not give any Personal Information and you may not sign up for or participate in any aspect of the Service.	Yes	Self-declaration	Date of Birth
Call of Duty	Subject to any applicable age rating or other	Yes	Self-declaration	Date of Birth

	restrictions, you may establish an Activision account only if (i) you are 18 years of age and a "natural person" in your country of residence, or (ii) if your parent or guardian reads and accepts the terms of this Agreement and the Activision Privacy Policy on their and your behalf if you are aged 13 or over but under 18 years of age. It was not possible to create an account for a minor.			
Clash of Clans	According to the Terms of Service, to use or register for an account you need to be the legal age of majority in your country of residence. If not, your legal guardian must review and agree to the Terms of Service.	We have not been able to establish if and when the age of a player is verified.	We have not been able to establish if and when the age of a player is verified.	We have not been able to establish if and when the age of a player is verified.
FIFA	According to the EA User Agreement you have to be at least 13 years of age (or the minimum age of your country of residence) to create an EA Account. Children under the age of digital consent can have a "child account".	Yes	Self-declaration	Date of Birth
Fortnite	According to the Epic Game's Terms of Service you must be an adult or the legal age of majority in your country of residence to enter into the contract.	We have not been able to establish if and when the age of a player is verified.	We have not been able to establish if and when the age of a player is verified.	We have not been able to establish if and when the age of a player is

				verified.
Grand Theft Auto	Age is not mentioned in the Terms of Service. As a minor you are not able to enter the GTA website. You can create an account for the Rockstar Games Social Club through the general Rockstar Games website when you are 14+.	Yes	Self-declaration	Date of Birth
League of Legends	To be eligible to create an account and use the services you either must be an adult or have permission from your parent or legal guardian. *However, you can create an account for 13+.	Yes	Self-declaration	Date of Birth
Roblox	Children under the age of 13 are able to create a Roblox account, which will automatically be set to “Privacy Mode”.	Yes	Self-declaration	Date of Birth
Apple	For an Apple ID you must be 13 (“or equivalent minimum age in your home country as set forth in the registration process). Apple ID’s for persons under this age (child accounts) can be created by a parent or legal guardian by using Family sharing.	Yes	Self-declaration	Date of Birth
Google	Children of all ages can have an account, but children need parental consent to create an account.	Yes	Self-declaration	Date of Birth
Microsoft	There is no minimum age, but children under 13 years	Yes	Self-declaration	Date of birth

	old will be added to the parent or guardian's family group.			
Nintendo	There is no minimum age, but children under 13 years old need to have a "Child account".	Yes (at 2 separate stages of the account creation)	Self-declaration	Declaration (being over or under 16 years) + Date of birth
Playstation	7 (accounts for 7-17 year olds must be created by a parent)	Yes	Self-declaration	Date of Birth
Steam	The minimum age to create a Steam User account is 13.	Yes	Self-declaration	Declaration "I am 13 years of age or older" and "I am under 16 years of age or older".

6.3.2. Parental consent

If the child has not yet reached the age of digital consent, the parent or someone else who has responsibility for the child must give consent on their behalf. In order to establish that it is indeed the parent who gives consent, some verification of their position as a parent will have to take place. As we are investigating consent mechanisms in this analysis, it is relevant that consent is one of the lawful grounds. Only apps, games and platforms where this is the case are therefore part of the analysis. Furthermore, we found that children are accepted in the digital services we examined. Usually a limit is drawn at children from 13 years of age who can apply. For some countries, this is the age of digital consent, but in other EU Member States, a different and therefore higher age of digital consent is used, and it will therefore be necessary to ask for parental consent. Furthermore, we have seen in the previous section on age verification methods that in most cases no effective way of age verification is used as this is usually done by self-declaration of date of birth or age. We will return to this in the assessment of the findings, however, we assume that parental consent is also required for children under 13 who are excluded by the digital services but who still actually use them.

In cases where children under 13 are excluded by the digital service, parental consent is not asked nor verified when signing up for a digital service. This is the case with Discord,

Facebook[22], Pinterest, TikTok, Twitter[23], Youtube, Yubo, Among Us, Call of Duty: Modern Warfare, Clash of Clans, Fifa, League of Legends, and Steam. If apps or games use the age of 13 as the cut-off age for age gating, the privacy policy may still state that a different age applies if the age of digital consent in the child's country is higher than 13 or simply refer to the age of digital consent under the law of the country of the user. So e.g. children under 16 may not use a service when the age of digital consent in their country is 16. This is the case with Discord, Pinterest, Twitter, Fortnite. In League of Legends, however, you can register if you are under the age of digital consent but over 13. The child must enter the parent's email address and the parent will receive a message with the option to approve the account (yes, let my child proceed). However, parental consent is not specific during the application phase, nor does it seem to verify that it is the parent who gives consent.

In some cases, it is not stated in so many words that children under 13 (or another age if the applicable law stipulates a different age of digital consent) are being excluded, but personal data relating to those children are stated not to be knowingly processed. In fact, that is like excluding that group of children but the implementation may be different. Twitch states that they do not knowingly process personal data of users under the age of digital consent and parental consent is not asked. Grand Theft Auto (GTA) also states that they do not knowingly process personal data of children under 13 (or older if that is the age of digital consent under applicable law), but if some services are nevertheless targeted at those children, data processing may be restricted or parental consent requested. If they discover that parents have not given their consent to data processing, the data will be deleted. However, we did not come across a parental consent mechanism when signing up to GTA.

Moreover, Clash of Clans is also not aimed at children under 13, but because the game is attractive to that age group, there are special settings for them (limited social media and chat feature, data processing only for internal service operations). However, there is no age verification during game sign-on and we did not find any parental consent mechanism either, so it is not clear if and when they apply these settings. Fortnite says it has a parental approval process for children under 13 ('COPPA minor') where a child account is created. A parent-authorised child account does not appear to be different from a normal account, except that parents are given information about parental control options. However, we did not come across a parental consent mechanism in our research. Roblox allows children under 13 to sign up but their accounts are set in 'private mode'. This means that social media plugins and third party advertising are not accessible. Children are allowed (not required) to provide an email address of their parents, after which parents are informed about the account, the settings can be reviewed and the account approved. The parent receives an

[22] Facebook uses 14 years as the minimum age to sign up in Spain and South Korea.
[23] For Periscope the minimum age was 16 but this service has been discontinued as of 31 March 2021.

email from Roblox and can agree to their child's account by clicking a link 'I Agree, Verify Email', which is not a specific parental consent for data processing. Moreover, it is not verified whether it is indeed the parent (or another legal guardian) who gives permission to the child. In the case of Apple, children under 13 (or the age of digital consent) can obtain a child Apple ID via their parents.[24] To give permission, the CVC code of the credit card associated with the parent's account must be entered. However, there is no actual verification that the person creating the child's Apple ID is the child's parent (or other legal guardian). Although, it is assumed that the person is over 18, as they must have a credit card. Furthermore, no parental consent is given for specific processing purposes, as agreement to the Terms and Conditions is all that is required.

For Google, too, a parent or legal guardian must be involved if children under 13 (or older depending on the age of digital consent in the child's country) want to create an account. After ticking a box that they consent to the processing of their child's personal data (incidentally, not a specific consent in the sense of Article 6 GDPR), the parent must log in to Google with their account to confirm this consent and agree to the creation of the account by the child (the latter not being the same as parental consent under the GDPR). Google then states that they will verify the Google account of the person giving consent for the child account to determine if that person is the parent. They say they do this by checking "account details, like your age, payment history, and how you use certain Google services", which does not necessarily say anything about whether this person is the parent. The parent can then choose either 'express personalisation' or 'manual personalisation'. In the first case, the parent receives quite detailed information about the processing of the child's personal data with the aim of personalising the service. After that, the parent has to click 'confirm' again to agree to the personalisation that is turned on by default in this option. According to Google, the settings can be adjusted later in the account settings. In the second case, the personalisation settings can be set (including switched off) more specifically. The child's account is linked via Family Link to the parent's account and the parent is thus given the possibility to set parental control settings. Interestingly, the process for creating a child account has changed over the course of this analysis. Whereas in the previous process (March/April 2021), the child had to enter their password to link the child's account to the parent's account and confirm that "you and your parent have both reviewed what monitoring means and want to link your accounts", now the child is only informed that parents can use Family Link. In the case of YouTube Kids, parents must sign in with their own Google account and provide their year of birth which is not checked based on the Google account.[25] The parent must then agree to the privacy policy, but there is no consent for

[24] There is also the option of a managed Apple ID that can be requested by schools but we did not explore this further in this study.
[25] We specified a different year than the one stored in the Google account with which we created a YouTube Kids account.

specific processing purposes.[26] The option to adjust the settings of the app is parents only based on a capacity test that asks the answer to a mathematical sum (e.g. 7 x 8 = ?) but this concerns parental control settings and not privacy settings.

Furthermore, a child account for children under 13 (or the applicable age of digital consent) can also be created at Microsoft, which - apart from requiring parental permission and allowing parents to manage consent choices and privacy settings - functions like any other Microsoft account, though it is stated in Xbox's privacy policy that privacy settings for these children are more restricted. Microsoft indicates that children under 16 will not see personalised ads and can turn this option on when they turn 16. So they choose the safe option under Article 8 GDPR and wait until the child has definitely reached the age of digital consent, which means they are also not dependent on parental consent for such data processing. The account is also used to create an Xbox profile. The parental permission process is activated by entering the parent's or guardian's email address in the login process after which the parent must log in with their own Microsoft account to give permission for a child account to be created. The information screens provide information about the processing of the child's personal data for various purposes but it is not clear which processing is based on consent and the screen asks for consent for the child account (not specific data processing). Then, the parent must fill in their name as specified for a Microsoft account to confirm that they are the parent or guardian. We found no evidence that this is further verified by Microsoft. The parent is then given an opt in to allow children to sign in by third party apps but even this choice is not sufficiently specific nor informed to potentially constitute consent under the GDPR.

In the case of Twitter, if anyone under the age of 13 or the age of digital consent tries to sign up, the account is locked and can only be reactivated after parental consent has been obtained. Parents have to fill in a form and it can take up to 60 days before a request is processed. Parents must provide their name and email address, their child's name and Twitter username, and a copy of a valid government-issued ID,[27] and proof of legal guardianship[28]. According to Twitter, these documents will be kept confidential and deleted after confirmation of identity and date of birth. Moreover, parents must by ticking boxes confirm responsibility over the child and agree to processing of their child' personal data pursuant the Terms of Service, Privacy Policy and Cooky Use policy. Only Twitter has a verification method that requires proof of parenthood or guardianship, or at least from which parenthood can be inferred, as in addition to an official ID, proof of legal guardianship

[26] There is only a very general statement in the privacy policy that says, "We share information from individual users with companies, organizations or individuals outside of Google with parental consent."
[27] E.g. driver's license, passport, or birth certificate.
[28] E.g. power of attorney, birth certificate, documents showing parental/guardianship rights over minor children. The uploaded document needs to be a legible copy with the child's full name and date of birth completely visible. See https://help.twitter.com/forms/parental_consent (accessed April 2021).

must also be provided. However, consent to the privacy policy by the parent is not a specific consent as required under the GDPR. Twitter also locks the account if the child is over 13 but under the age of digital consent. An email address of the parent must be provided which is then redirected to a site where parental consent can be given. The full name of parent and child, Twitter username child, email address parent, copy of valid government-issued ID to confirm identity parent (e.g. driving licence, passport, birth certificate, etc.) or, in case of guardianship, documents showing that the guardian may act on behalf of the child (e.g. power of attorney, birth certificate, documents showing authority as parent or guardian over minor children and including child's date of birth) must be provided. Twitter is the only digital service where legal guardians are not only mentioned but also have to present documents to prove their status. Twitter declares that the documents will be treated confidentially and delete them after the verification process is completed.

In the case of Fifa, parents with an account can set up an account for their child when they have not reached the age of digital consent. This account will be converted into a teen account until they turn 18, when they have reached the age of digital consent. In the first situation, the parent must create an account through Origin, specifying the country and date of birth of the child and providing the email address linked to the parent's account. By ticking a box, the parent agrees to be the child's parent or guardian and to the privacy policy and transfer of their child's personal information to the United States. A password must be entered that the child will use for their Public ID. Anyone can in fact pose as the child's parent or guardian.

League of Legends asks for parental consent when an account is created by a child who is under the age of digital consent. The child receives an email saying parental approval is pending. An email address for the parent must be provided upon which the parent receives an email to approve the signup (asking whether the child can proceed or cannot proceed), however, no specific parental consent is asked.

Nintendo uses the age of 16 for parental consent sign-ups, with which the company seems to have opted for the safe option so that they always comply with Article 8 GDPR. If a child of 15 or younger signs on, they must call a parent to create a child account. The parent must also have an account or create one if they do not already have one. Among other things, they must enter their date of birth and email address and will then receive an email with a verification code that must be entered in the login process. The parent must share the following personal information about the child while creating the child account: desired nickname, sign-in ID, desired password, date of birth and gender. Both of these first data can then be shared with the child when the account is created so they can sign in. There seems to be no further verification of whether the person who registered the child is in fact the parent. The child's account contains the message in the settings that "A parent or guardian in

your family group has applied the following to this account: Restrictions on sharing of your account information (parent/guardian confirmation required each time).” The child cannot change the settings by themselves, only through the account to which the child account is linked.

At Playstation, all children (persons under the age of 18) have a child account that is linked to the parent or guardian's account. In order to add the child, the parent's home address and online ID, child's date of birth, email address and password for the child must be provided by the parent. Playstation then informs the parent about the privacy settings that the child can adjust, but no parental consent is asked for this (parents are only encouraged to help their children choose the appropriate settings). However, they can directly set parental control settings for their child.

In Steam, you can create an account by entering your email address, country of residence and so on. If you've specified being over 13, you're still given the option of being 16 or over or under 16, which Steam seems to have chosen for the safe option with regard to Article 8 GDPR. Parental consent is requested via the email address of the parent or guardian. Steam indicates that the information (parent/young person under 16, email address of parent) is not stored. The parent will receive an email with a link to approve their child's account, after which the child will receive an email saying that the login process can be completed. There seems to be no actual verification of parent or guardian status.

Some digital services have a special arrangement for children of 13 and over. Snapchat specifically states that they make reasonable efforts to seek parental consent from children between the ages of 13 and 16. However, parental consent was not sought for opening an account for a person under the age of digital consent. Although Yubo is also specifically intended for 13-17 year olds, and although Yubo says that parental consent is needed in their case, parental consent is not asked in the registration process. Yoti used for age verification within Yubo does not yet have a parental consent mechanism and can therefore only be used by children who have reached the age of digital consent.[29] With Among Us, children aged 13 to 18 must have parental consent before providing personal data, however, we have not found a parental consent mechanism. League of Legends allows children over 13 to sign up, but parental approval is needed if the child is still under the age of digital consent (in our case signing up as a 15 year old from a country where the age of consent is 16 parental approval was required, whereas signing up as a 13 year old from a country where the age of consent is 13 it was not. Parental approval means that the parent gets an email with a link that says 'yes, let my child proceed' which is not a specific parental consent. Moreover, it is not verified whether it is indeed the parent (or another legal

[29] In the message that the app gives you if you try to use Yoti when you are still of digital consent age, it says that they are working on a parental consent mechanism. It is not clear when that will be ready.

guardian) who gives permission to the child. TikTok has a separate privacy policy for children between 13 and 18 and their account is set to private by default but parental consent is not obtained.

In some cases, the app or game requires children to have their parents or others with parental authority to review the terms and conditions. This is the case with Discord[30] and Call of Duty: Modern Warfare, and Fifa. Since this is about entering into a legal agreement and consenting to the terms of Service (including the privacy policy), rather than consenting to data processing for a specific purpose, it falls under contract law and not data protection law.

Even when parental consent is not asked when setting up an account, which is when the approval of the parent during the creation of an account does not meet the requirements of the GDPR or if no parent is involved at all, the privacy settings may still require parental or guardian approval for specific data processing.[31] In this way, specific consent is still requested and certain personal data are not processed for certain purposes until such consent is given. This is the case with Facebook where such a request for parental consent requires entering name (when they themselves have a Facebook account) or e-mail address of the parent or guardian. Upon receiving the request, they can approve or decline by providing their name, date of birth and ticking the box 'I am authorized to approve' and clicking approve or decline all. Also, Instagram asks for permission from a parent or guardian to see "better ads" (i.e. personalised ads) in the case of children not having reached the age of digital consent. Parents/guardians will receive an email and can then approve or decline upon entering name, birth date and stating they are authorized as a legal guardian by ticking a box. They can also let Instagram know when they are not the parent/guardian. Any changes to the approval must be requested with a dedicated form. Clearly, in these cases parental consent is based on self-declaration and, as far as we could see, not further verified by these digital services.

In France, joint consent of parent and child is necessary if the child has not yet reached the age of digital consent. You could argue that in cases where parents confirm the choice of certain privacy settings by children, as in the case of Facebook, there is joint consent. Legally, at least in countries that do not have joint consent, only parental consent will be considered as lawful consent to data processing. In the case of Yubo, the processing of location data is explicitly subject to the consent of the child and the legal guardian.[32] However, if and how this joint consent is obtained is unclear.

[30] The Privacy Policy fails to explicitly specify what this consent relates to in particular. It states: "Where required by law, and in some other cases, we handle personal data on the basis of our implied or express consent".
[31] Note that we have not documented how easily accessible privacy settings are, however, based on the principle of transparency, choices should be easily accessible.
[32] See https://yubo.live/en/legal/privacy under "What data do we collect" (accessed April 2021).

In the following table some of the findings concerning parental consent mechanisms in the apps/games/platforms are summarised[33]:

Apps / Games / Platforms	Parental involvement required?	When?	How?	Specific Parental Consent?
Discord	No	N/A	N/A	N/A
Facebook	Yes	When the child manages their data settings with regards to "ads based on data from partners" (personalised ads) and "specially protected data in your Facebook profile".	The parent / guardian receives an email, after which the parent has to enter their first and last name and date of birth and tick the box to declare "I am authorised to approve XXX's choices as a legal guardian".	The parent is presented with and asked to approve the data choices made by the child.
Instagram	Yes	When you sign up as a 13 year old, you are prompted to ask a parent or guardian for their approval to "see better ads". This step can be skipped.	The parent / guardian receives an email, after which the parent has to enter their first and last name and date of birth and tick the box to declare "I am the legal guardian of XXX and am authorised to approve their data choices".	The parent is presented with the information that the child wants to see personalised ads and is asked to approve.
Pinterest	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Snapchat	Even though mentioned in Snap's privacy policy, in our	N/A	N/A	N/A

[33] For the complete results of the performed case study research please see the Technical report in Annex 1

	test cases (Portugal and The Netherlands) no parental consent mechanism was activated.			
TikTok	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Twitch	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Twitter	Yes	At account creation. When a child older than 13 years, but under the age of digital consent signs up, the parent / guardian needs to give parental consent to unlock the child's account.	The parent / guardian must provide their full name, the child's full name, the Twitter username of the child, email address of the parent, copy of valid government-issued ID to confirm the identity of the parent or in case of guardianship, documents showing that the guardian may act on behalf of the child. It is required to tick a box to confirm that you hold parental responsibility over the child. Also the parent / guardian has to declare to have reviewed the child's account and agree to	No

			Twitter using their child's information, in the ways described in Twitter's Terms of Service, Privacy Policy and CookieUse.	
YouTube / YouTube Kids	YouTube: see Google YouTube Kids: Yes	YouTube: see Google YouTube Kids: after installing the app	YouTube: see Google Youtube Kids: whether you choose to sign in with your (Google) parent account or to continue without doing so you are presented with information regarding the data processing of children after which you have to enter your password to confirm or click "I Agree".	No
Yubo	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Among Us	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Call of Duty	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Clash of Clans	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A

FIFA	Yes	At account creation. A child's account can only be created via the EA account of the parent / guardian (their email address is used to set up the child's account).	The parent / guardian declares that they are the parent / guardian of the child using the account, and that they accept the User agreement and understand that EA's Privacy and Cookie Policy applies to their child's use of EA's services. Once the account is created, the parent receives an email with instructions to activate the account.	No
Fortnite	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
Grand Theft Auto	No evidence was found of any parental consent mechanism.	N/A	N/A	N/A
League of Legends	Yes	When a child older than 13 years, but under the age of digital consent signs up, the parent / guardian needs to approve the account.	The parent receives an email in which the parent has to choose to let the child proceed with the account creation or not.	No
Roblox	Yes	Children are allowed (not required) to provide an email address of their parents in their	When a child enters their parent / guardian's email address they are informed about the account, the settings	No

		account settings (once the account is already active).	can be reviewed and the account approved.	
Apple	Yes	At account creation. A child's account (for children under the age of digital consent) can only be created via Family sharing.	The parent has to click "Agree" to consent to Apple's collection, use and disclosure of your child's information as set forth in Apple's Privacy Policy. To confirm you have to enter the security code (CVC) for the credit card associated with the parents / guardians Apple ID.	No
Google	Yes	At account creation, when the child has indicated to be under the age of 13 (or the "applicable age in their country").	The parent has to give permission to the account creation of the child and the processing of the child's information as described. The parent has to login their Google account and by entering their password, they confirm that they agree to the parental consent and that they want to create the child's Google Account.	After providing a general parental consent, the parent can personalise the child's data settings.
Microsoft	Yes	At account creation, when the child has indicated to be under the age of digital consent.	The parent (or guardian) has to give permission to create the Microsoft account for the child, accept the Services Agreement and Privacy Statement on behalf of the child, and authorize the	No

			collection, use and disclosure of info about the child through Microsoft's online services, products, and apps by providing their e-signature. After, the child's account is added to the parent's family group, in which parental controls can be managed.	
Nintendo	Yes	At account creation, when the child has indicated to be aged "15 or under".	A child account can be created and managed through a parent's or guardian's account. At the last step setting up the child's account the parent / guardian declares to (on behalf of the child) agree to the terms and acknowledge the Nintendo Account Privacy Policy.	No
Playstation	Yes	At account creation, when the child has indicated to be under the age of 18.	The parent has to have a PSN account, after which the parent can add the child as a family member (create the account) and set parental controls. Information is given with regards to handling of data of their child's account, which the parent needs to agree to by clicking "confirm".	No
Steam	Yes	At account creation, when the	An email is sent to the parent / guardian to	No

		child has indicated to be under the age of 16.	ask for permission to create an account on the Steam platform. After clicking on the hyperlink "Approve" the child can complete the account creation process.	

6.4. Assessment of consent and age verification mechanisms

This section will provide an assessment of the results of the study of the selected apps/games/platforms based on the analysis from Section 6.3. First we will discuss age verification and then parental consent methods from a data protection and children's rights perspective respectively.

6.4.1. Age verification

6.4.1.1. Assessment from a data protection perspective

The research shows that the most commonly used method of age verification is self-declaration. This may be a suitable method if low-risk processing is involved. Although we have not specifically investigated the extent to which the criteria for high-risk processing (such as monitoring of online behaviour and profiling of users) are met, it does seem plausible to assume that there is high-risk processing, given that the high risk criterion of processing personal data of vulnerable persons, namely children, applies in any case.[34] Moreover, data processing for which consent is given by children under the age of digital consent is not lawful. Self-declaration thus does not seem to be an adequate form of age verification.

This is all the more the case since there is an incentive for many children who sign up for a digital service to give a date of birth or age other than their actual date of birth.[35] Children under 13 (or other applicable age of digital consent) are not supposed to sign up to many of the apps and games in our analysis because they have not reached the minimum age set by these companies. The minimum age seems to be based on the minimum age for

[34] This is all the more so given that any activity impacting a child also triggers the application of the best interest principle (Article 3 CRC) which requires digital service providers to consider the welfare of children in the design and use of their services.
[35] See also D2.4 on Age verification, parental controls and parental consent in everyday life: A rapid evidence review, Doc. Version 0.1, p. 26, pointing out that parents help children to circumvent age restrictions.

digital consent in COPPA and the GDPR (including, where applicable, the variations defined by EU Member States). Although companies have the freedom to determine with whom they do business, this practice seems to be mainly aimed at circumventing Article 8 GDPR and thus the requirement of parental consent. However, a gratuitous statement that the service is not intended for children is not sufficient and processing of personal data based on consent by a child who has not reached the age of digital consent will, as mentioned, be unlawful.

Only Yubo, which is specifically aimed at teenagers, has an age verification method that goes beyond self-declaration by using the age verification services of Yoti. The limitation is that only children who have reached the age of digital consent can use Yoti. So that leads to quite significant differences in the EU due to different national implementations of Article 8 GDPR. In addition, there is the underlying problem that this consent is needed because they are processing (potentially) sensitive personal data, biometric data in their own words, and it is open to question whether this is the most privacy-friendly solution. Children who cannot use Yoti can send Yubo three photos, one of which also shows the child's ID (or school card). What is not clear is what happens if you do not verify your age (Yubo talks about identity by the way, which is not the same). You don't get a yellow 'verified' badge on your profile but we could still use the app. In that case, age verification in Yubo is no different than other apps that only use self-declaration. Only after some time (more than a month) did Yubo send a message that the (our non-verified) account could be blocked if there was any suspicion that it was a fake account.[36] Yubo says it will verify the age and identity. As of yet, we have not received a verification request and the reference to a fake account seems to indicate that it is not about verification in the sense of the GDPR but about the safety of children.

Only where a digital service is restricted to 18 and over, and there is no evidence that children are using it anyway, does the special protection that children should receive under the GDPR not need to be taken into account. This requires an adequate form of age verification, which we found in almost none of the apps and games. As mentioned, Yubo has advanced age verification but we could still use the app without it.

With the exception of Yubo, none of the other apps showed the use of a third party to verify the age of users. A trusted third party can actually be interesting for implementing a privacy-friendly age verification method. The app then does not need to process personal

[36] This is what the message says: "We do everything we can to protect you guys.
Fake profiles are against our community guidelines, and they can put you at risk. Yubo is all about making friends, so it means we need to make sure that whoever you talk to, that person is actually real.
We use a combination of artificial intelligence and human brain to detect and lock accounts suspected of being fake until their age and identity are verified. If your account is locked, you'll probably be annoyed and we understand that. Bear with us a bit, and your account will be unlocked super quickly."

data itself to verify the age, but only receives an answer, for example, that the child is under or over a certain age. Especially if the method works with age tokens that are stored on the child's own device, this is a privacy-enhanced method that minimises the processing of personal data. However, this is not the method used by Yoti as they still require the user to show ID, among other things, and they also use a face scan which is potentially a form of biometric data (and therefore special personal data under Article 9 GDPR). None of the apps and games thus seem to have sought a privacy-enhanced solution for age verification, with the exception of Steam which only asks whether a child is under 13, or under or over 16 and says not to save this information. However, this does raise the question of the extent to which companies can meet their accountability obligation under the GDPR if the results of the verification process are not stored unless it can be proven otherwise that there was integrity in age verification. Moreover, ironically, with the low assurance age verification method of self-declaration little personal data is processed anyway and the user also has the option of providing false data that obscures the actual age. Finally, it seemed that apps and games were using location data as they usually automatically knew which age of digital consent applied when signing up. However, we were not specifically told that this was happening. This is another process that could potentially be made more privacy-enhancing by using a third party to verify on the user's device which age of digital consent applies without sharing location or country of residence.

6.4.1.2. Assessment from a children's rights perspective

It is in the child's interest that their fundamental right to data protection is respected in a way that is appropriate and adequate for them. The implementation of the age verification obligation in relation to children (all children and not only those who have not yet reached the age of digital consent) in the GDPR still leaves much to be desired as we have seen in the previous analysis. This means that it is impossible for companies to guarantee that individual children receive an age-appropriate experience and child-friendly privacy settings. It would potentially be different if the digital services analysed in this study had a by default age-appropriate and privacy-enhanced character, because in that case they would be suitable for all users from a data protection perspective. It is incidentally true that some apps have privacy-friendly settings by default (e.g. an opt-in for personalised ads[37]), but this of course only works if the age verification is adequate.

In cases where a more advanced form of age verification has been implemented, we see that traditional IDs (or similar documents) are often still required. Not only is that generally not a privacy-friendly way of age verification, but it also means that only children who have those documents can register. This may exclude groups of children from these

[37] By the way, the question is whether you should give children the option to see personalised ads at all, but that is a matter beyond the scope of this study.

digital services. One of the apps concerned, Yubo, does indicate that you have another option if you do not have an ID, but it was not clear to us what that option is. Now children were not actually excluded here because it seems that you can also use the app without verification but, as mentioned, that again raises the previously discussed data protection and child rights issues and is not an adequate situation either.

6.4.2. Parental consent

6.4.2.1. Assessment from a data protection perspective

As the analysis in 6.4.1.1 showed, children can easily bypass the age verification that digital services have implemented, which means that there is no parental consent when this is required under Article 8 GDPR. As a result data processing based on consent as a lawful ground for children under the age of digital consent is unlawful and this is the case with most, if not all, of the apps we have analysed as part of this study.

However, assuming that children do enter their age correctly and are allowed to make an account when under the age of 13 (or the applicable age of digital consent), there are apps stating they ask for parents to approve the account. Yet in many cases we did not come across a parental consent mechanism. In cases where a mechanism was built in to involve parents in the application process, this was usually based on an email address of possibly the parent or a guardian. So there was no actual verification whether the parent or someone else (possibly even the child themselves) approved the account. However, the method can provide sufficient assurance if there is low risk data processing. As indicated earlier, we have not specifically examined this in our research but the fact that personal data of children is being processed is considered to be a reason to assume that the processing is of a high risk nature.

Other methods we found, such as the use of a credit card by the parent or linking the child's account to a parent's account, do not actually verify whether the person in question is the child's parent. In the case of credit card verification, it may be possible to assume that the person is of age, since you can only apply for a credit card if you are 18 years old. Only Twitter has a verification method that requires proof of parenthood or guardianship, or at least from which parenthood can be inferred, as in addition to an official ID, proof of legal guardianship must also be provided. However, this can be circumvented by signing up immediately with an age higher than the minimum age required by Twitter or restarting the sign-up process after the previous one has been locked. Although some apps mention guardians as well as parents, guardianship is not specifically verified.

In most cases where parental approval is sought it is quite general and does not constitute consent to a specific data processing activity as required by the GDPR. It does happen that there is information about the specific purpose of the data processing for which consent is given in the privacy policy but then there is no choice other than to agree to the policy and thus consent is not freely given. Some apps, however, ask for parental consent when the child changes the privacy settings which may constitute specific and free parental consent (which then obviously still needs to be informed as well). The verification of the person's status as a parent or guardian is then done on the basis of a self-declaration and it is not said that it is indeed the parent (or an adult) who is consenting.

From a privacy by design perspective, it is relevant that Twitter as one of the apps seriously attempting to verify parental (or guardian) consent does require potentially privacy invasive information (ID/birth certificate/proof of guardianship), although they say that the documents will be treated confidentially and deleted after the verification process is completed. In itself, it is understandable that they have chosen this method because it is difficult to think of another way to prove parental authority or guardianship but with traditional documents. A privacy-friendly option might, however, be when the parent can use an electronic ID to verify parental authority with the government administration in a decentralised way, i.e. data is processed only on their device and no more than a yes (is the parent) / no (is not the parent) answer is given to digital service provider. In our research we did not investigate whether these methods exist. For the time being, the use of a credit card is therefore an interesting option because you can then, in principle, assume that the person verifying is at least an adult (and older than the age of digital consent). The disadvantage is that not every parent has a credit card and children can therefore be excluded (if and when age verification methods become more effective).

We have seen no evidence of trusted third parties being involved in the verification of parental consent.

6.4.2.2. Assessment from a children's rights perspective

When children are not yet able to consent to specific data processing, it is important that parents (or guardians) can do so for them. Parents are primarily responsible for their children and are expected to act in their best interest. Parents may also be in the best position to determine what their children understand when it comes to data processing. At least in theory, because it may not always be very clear to parents themselves how apps and games handle their children's personal data. And although we have seen in this study that data processing requiring consent as a lawful ground is limited, it is expected that the more

data-driven (and therefore more complex) practices (e.g. targeted advertising[38]) will require consent.[39] It is therefore important that parents (and preferably children themselves) are properly informed when parental consent is given in order for them to be able to adequately exercise their responsibility as a parent. If data processing is too complex to explain, especially to children, you have to ask yourself whether you should do it at all.

The study shows, however, that what is claimed to be parental consent often is not in the sense of GDPR. Not only can age verification and parental consent be easily circumvented by children, but consent to data processing can simply be given by someone other than the parent (and parental controls set, since the two are not always separated). Earlier, we raised the question of whether it might not be sufficient to ask the consent of an adult without it necessarily being clear whether that is the parent or guardian. The reason is that adequate and privacy-friendly methods of age verification may be easier to develop than methods of verifying parental authority. However, we are aware that this is at odds with the primary responsibility of parents under Article 18 CRC. At the same time, a distinction must be made here between parental consent and parental control; in the latter case, parents of young children certainly want to be involved in the use of apps and games. One possibility is perhaps to interpret parental consent more broadly in the case of teenagers and to permit consent by adults (not necessarily parents). This has the advantage that teenagers who prefer not to involve their parents (e.g. because the relationship with them is not particularly good or their app use may reveal something about their lives that they find too sensitive to share with them) have other options for consent. However, such an interpretation is not very directly supported by the wording of Article 8 GDPR.

As mentioned earlier, the relationship between parent and child can be such that children prefer not to involve their parents in signing up or using an app. For example, allowing the parent to create a password for the child's account and to view the privacy settings very directly can be a suitable method for younger children. With older children and teenagers in particular, a method could be used in case of data processing for which parental consent is required whereby the parent can assess the nature and extent of the data processing by the digital service provider (e.g. in the parent's own linked account or via an email message) but cannot see what else is happening in the account. We saw both forms in the study. In any case, it is relevant to take the interests of the child, their evolving capacities and the impact on their children's rights in a broad sense (also including their participation rights) into account when designing the parental control mechanism. The way to do this is to conduct a child rights impact assessment involving children themselves.

[38] By the way, the question is whether you should give children the option to be confronted with targeted ads at all, but that is a matter beyond the scope of this study.
[39] As mentioned earlier (section 5.3.), eliminating privacy invading data processing which generally requires consent can avoid triggering the application of Article 8 GDPR on children's age of digital consent and hence the requirement of parental consent if applicable.

In terms of impacting children's rights beyond data protection, it is also important that consent mechanisms are inclusive. Given that (effective) parental consent (and age verification) mechanisms were mostly not in place or parental authority not actually verified, the problem does not arise now, but children must be prevented from being excluded because their parents or guardians are not available or verification of their authority is not possible. And other factors that may lead to exclusion, such as language or disability, must also be taken into account.

Finally, it is important that age verification and parental consent methods are transparent for both parents and children. Transparent in the sense of Article 12 GDPR so that parents and children know which data is processed how and for how long. But it must also be transparent to children how parents are involved in the process so that they understand what parents see from their online activities. As indicated earlier, there must be a clear distinction between parental consent (a legal act with the aim of giving consent for a specific data processing) and parental control (tools or strategies to guarantee the safety of children beyond data processing). In the first case, Article 8 GDPR (and the concrete implementation of that provision in the EU Member States) is leading, in the second case it depends on the evolving capacities and the best interests of the child to what extent it is justified for parents to be able to control activities. The latter is admittedly easier said than done, as parents have their own responsibility to determine this for their children, individual children may have different needs, and there may be broader cultural differences between countries, regions or groups in society. For this reason, it is essential as part of a children's rights impact assessment to involve not only children but also parents in the design and development of age verification and parental consent mechanisms given their potential use as a parental control tool. Moreover, this is not a one-off exercise, as the impact is often only apparent in the use of such tools. In any case, it is important to distinguish between parental consent and parental control, because in our analysis we saw that the division between the two was not always very clear. The same applies to the distinction between parental consent within the meaning of Article 8 GDPR and parental permission for the conclusion of a contract under national contract law, which are two different legal acts.

7. Conclusions

This study has mapped existing methods for age verification and obtaining parental (or guardian) consent in various apps and games that are used by children. Moreover, we have assessed how the age verification and parental consent methods in these apps and games that we have identified can be assessed based on the data protection and children's rights framework. The purpose of this study was not to do a full compliance check on what methods are used and how they have been implemented but to determine how they comply

with the directly relevant provisions in the GDPR, including Article 8 GDPR. Furthermore, we did examine how the methods relate to the principles of data minimisation and privacy by design, given that these are particularly relevant to the protection of children. The children's rights analysis then shows how the rights of the child as enshrined in the 1989 UN Convention on the Rights of the Child which are relevant to the design, development and use of apps and games used by children, trigger specific considerations with respect to the age verification and parental consent methods identified in the apps and games. In order to present our findings we return to research questions that we wanted to answer with our study.

- What methods are used for age verification and to obtain parental consent?

The method most commonly used in both cases is self-declaration. Clearly, these methods make it easy for the user to manipulate age verification (and, hence, circumvent parental consent if it is even present). There is an incentive for children under 13 (or applicable age of digital consent) to pretend to be older than the minimum age to sign up for digital services, otherwise they will be excluded from most services. Even when digital services say they ask for proof of age, it is not clear if and how this is done. Some digital services do not even ask for an age or date of birth, or they can be used without creating an account and therefore do not require age verification. There is one digital service that has a more advanced method of age verification built in, which is based on a third-party verification service (through face scan, photo and official ID) or, if the user is younger than the age of digital consent, by the service itself on the basis of three face photos, one of which also shows an official ID. However, we were able to use the app without this verification for the duration of the study.

If a child applies with an age below the age of digital consent and they are not age gated, then parental consent can be asked. Mostly this is also based on self-declaration with the child, for example, being asked to provide an email address of the parent (or guardian) who must then respond by giving the child permission to open an account. Although some services indicate that they ask for parental consent or have special settings for children under 13, we could not always find a parental consent mechanism. Where parental consent was requested (e.g. by linking the child's account to that of the parent), it was not actually verified as being the parent (or guardian). We found one exception though, where copies of official documents had to be provided to prove the parent's identity as well as parental authority or guardianship. While in most cases parental consent was requested in the sign up process, there were also examples where parents had to agree to change the privacy settings (e.g. if the child wants to turn on personalised ads, the parent has to approve).

- How do these methods comply with data protection laws?

Self-declaration for age verification can be an adequate method when it comes to low-risk data processing. Although we did not examine this specifically in the case of the apps and games in this study, we assumed that, given that children's personal data is being processed, methods that offer greater certainty would be necessary. And also because data processing for which consent is given by children under the age of digital consent is not lawful. Moreover, it is important to keep in mind that age verification is necessary also when no parental consent is necessary, given that the GDPR intends to offer protection to children (under 18s) and not merely to children that have not yet reached the age of digital consent.

The few times that digital services do use a stronger form of verification, it is mainly on the basis of traditional documents (such as passports or birth certificates) that contain more data than is necessary to verify age or parentage/guardianship and are therefore at odds with the principle of data minimisation. In principle, systems that return yes/no answers to the question of whether someone is under a certain age and whether someone has authority over the child, are more privacy-friendly than systems that process age or date of birth. Where such systems for the verification of parental consent are not available or difficult to develop, we have suggested at least adequately verifying whether an adult has consented to the processing of the child's personal data. However, such an interpretation is not very directly supported by the wording of Article 8 GDPR.

In the case where parents were involved in the application process, their approval did not meet the conditions for consent because it was often not aimed at data processing for a specific purpose. In most cases, it was simply a matter of ticking a box that said they agree with the privacy statement that covers all intended data processing. Interesting, however, was the option that was sometimes offered to parents to specifically agree to a particular data processing in the privacy settings of the child account. Again, however, verification that it is the parent who gives their consent was not watertight.

All in all, there is still work to be done to design and implement age verification and parental consent methods that comply with the GDPR and actually offer children better protection of their personal data. Particularly, the development of child-friendly and privacy preserving verification tools can contribute to this. This should also include the drafting of codes of conduct with guidelines (see also Article 40 GDPR), the development of standards, best practices and certification of methods and trusted third parties offering such child-friendly and privacy preserving verification methods.

- How do these methods comply with the children's rights?

The data protection problems described above can be avoided by designing and developing digital services that are child-friendly and privacy-preserving by default. This would be in the best interests of the child, a fundamental principle in the 1989 UN Convention on the Rights of the Child, which should always be the starting point when an activity has an impact on children. This applies not only to the apps and games we have studied but also to the verification methods used or to be developed.

From a children's rights perspective, it is interesting to mention again the option of seeking consent from an adult because it is difficult to verify (in a privacy-friendly way) that someone has parental authority. However, we realise that this is at odds with the primary responsibility parents have for their children (Article 18 CRC) and, presumably, their desire to be involved in the decision as to whether certain personal data requiring consent (usually the more data-driven activities) are processed. Such involvement of parents can then, of course, be easily circumvented by asking someone else of 18 and over to consent. From the point of view of children's evolving capacities, it could be said that this solution is more appropriate for older children, but since, as mentioned, these are more data-driven and therefore more complex and less easily understood activities, it is questionable whether the argument can be sustained. From the child's best interest point of view, as a company you should turn this type of data processing off by default for children in which case (parental) may no longer be necessary.

When designing and developing verification methods, it is important to involve children and parents so that their views, experiences, needs and wishes can be taken into account. For many teenagers, it is expected to be important that parental consent does not also mean that parents can look into their account or into their online activities. For younger children, this may be different and parents may want to be more involved in keeping an eye on their children's safety (for example, by using parental control tools). Parental consent is not the same as parental control; the former is a legal act and the latter a factual activity. It should be transparent to children what parents can see in relation to their account when giving consent, and preferably the privacy settings take into account that some teenagers limit this to visibility of the data processing for which consent is given, and others might be fine with giving parents broader access to their account.

Verification methods must be inclusive and children (or their parents) should not be excluded because they cannot meet the requirements set by the verification methods. A child rights impact assessment must identify the issues that may arise with regard to inclusiveness and how to prevent them. Here it may be relevant, for example, that children or parents may not have access to certain verification methods (e.g. eID or credit card) or that it is complicated in the personal context of the child to ask for parental consent. Special attention should be paid to making digital services (including age verification and parental

consent mechanisms) accessible to children who face specific challenges such as physical and intellectual disabilities.

Finally, it is strongly advised that age verification service providers perform a child rights impact assessment to determine how verification methods may impact children and children's rights and assess how to implement legal requirements and address any concerns by implementing age appropriate safeguards. It is essential to involve children and parents in the process because they themselves are best placed to indicate their experiences and expectations.

Annex 1: Technical report

https://docs.google.com/document/d/1uaroi784OsEiLWrolcoXAMNt0jCdTpx64bsOyfrMhPg/edit#

References

5Rights Foundation. 2021. "But How Do They Know It Is a Child? Age Assurance in the Digital World." https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

AEPD, and EDPB. 2021. "Joint Paper on 10 Misunderstandings Related to Anonymisation." https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

Alderson, P. 2008. *Young Children's Rights: Exploring Beliefs, Principles and Practice Second Edition*. Jessica Kingsley Publishers.

Article 29 Data Protection Working Party. 2008. "Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)." https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf.

———. 2009. "Opinion 5/2009 on Online Social Networking." https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

Billinge, G., Burgess, R. and Corby, I. (2021) EU Methods for Audiovisual Media Services Directive (AVMSD) and General Data Protection Regulation (GDPR) Compliance. Age Verification Providers Association.

boyd, d. 2008. "Taken Out of Context, American Teen Sociality in Networked Publics." PhD, University of California, Berkeley.

Caglar, C. and Nair, A. (2021) EU Member State Legal Framework. Birmingham: Aston University

Commission Nationale de l'Informatique et des Libertés (CNIL). 2020. "Contribution Concernant Le Sujet Des Droits à La Protection Des Données Des Enfants Dans Le Cadre Du Rapport Du Rapporteur Spécial Des Nations Unies Sur Le Droit à La Vie Privée (UNSRP) Auprès de La CDH." https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/privacy-child/NHRI-Ombusman-Commissions/4-CNIL-FR.docx.

Committee on the Rights of the Child. 2003. "General Comment No. 5 (2003) General Measures of Implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, Para. 6)." http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6Zd2%2fQRsDnCTcaruSeZhPr2vUevjbn6t6GSi1fheVp%2bj5HTLU2Ub%2fPZZtQWn0jExFVnWuhiBbqgAj0dWBoFGbK0c.

———. 2009. "General Comment No. 12 (2009) The Right of the Child to Be Heard." https://www.refworld.org/docid/4ae562c52.html.

———. 2013. "General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (art. 3, Para. 1)." https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

———. 2016. "General Comment No. 20 (2016) on the Implementation of the Rights of the Child during Adolescence." https://digitallibrary.un.org/record/855544.

———. 2021. "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital

Environment." https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t.

Council of Europe. 2012. "Council of Europe Recommendation on the Participation of Children and Young People under the Age of 18." https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046c478.

———. 2018. "Policy Guidance on Empowering, Protecting and Supporting Children in the Digital Environment."

Data Protection Commission Ireland. 2020. "Children Front And Center: Fundamentals for a Child-Oriented Approach to Data Processing (Draft Version)." https://dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf.

European Commission. 2020. "Communication from the Commission to the European Parliament and the Council on Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

European Data Protection Board. 2020. "Guidelines 05/2020 on Consent under Regulation 2016/679." https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

Hoepman, J. 2020. "Privacy Design Strategies (The Little Blue Book)." https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

Hof, S. van der. 2017. "I Agree... Or Do I? - A Rights-Based Analysis Of The Law On Children's Consent In The Digital World." *Wisconsin International Law Journal* 34: 409–45.

Hof, S. van der, and Lievens, E. 2018. "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR." *Communications Law* 23 (1): 33–43.

Hof, S. van der, Lievens, E., and Milkaite, I. 2019. "The Protection of Children's Personal Data in a Data-Driven World: A Closer Look at the GDPR from a Children's Rights Perspective." In *Monitoring Children's Rights in the Netherlands: 30 Years of the UN Convention on the Rights of the Child*, edited by Liefaard, T, Rap, S, and Rodrigues, P. Leiden University Press.

Hof, S. van der, Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T, and Liefaard, T. 2020. "The Child's Right to Protection against Economic Exploitation in the Digital World." *The International Journal of Children's Rights* 28 (4): 833–59.

ICO. 2020. "Age Appropriate Design Code." https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.

Kwantes, E. 2017. "Dutch Youth and Experts on the GDPR."

Lievens, E., Livingstone, S., Mc Laughlin, S., O'Neill, B., and Verdoodt, V. 2018. "Children's

Rights and Digital Technologies." In *International Human Rights of Children*, edited by Kilkelly U. Liefaard T, 487–513. International Human Rights. Springer.

Lievens, E., Livingstone, S., McLaughlin, S., Brian O'Neill, B., and Verdoodt, V. 2018. "Children's Rights and Digital Technologies." *International Children's Rights Law*, 487–513.

Livingstone, S., Stoilova, M., and Nandagiri, R. 2019. "Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review." London: London School of Economics and Political Science.

Milkaite, I., and Lievens, E. 2020. "Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies." *Journal of Children and Media* 14 (1): 5–21.

Milkaite, I., and Lievens, E. 2019. "Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU." https://www.betterinternetforkids.eu/nl/practice/articles/article?id=3017751

Mukherjee S., Pothong K., Livingstone, L. 2021. "Child Rights Impact Assessment: A tool to realise child rights in the digital environment." London: 5Rights Foundation.

Nash, V., O'Connell, R., Zevenbergen, B., and Mishkin, A. 2013. "Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry." https://www.oii.ox.ac.uk/archive/downloads/publications/Effective-Age-Verification-Techniques.pdf.

Santos Silva, M. 2021. "Brief Reflections on Freedom of Contract and Paternalism in the Digital Era." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3759967.

Schermer, B.W., Custers, B., and Hof, S. van der. 2014. "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection." *Ethics and Information Technology* 16 (2): 171–82.

Shmueli, B., and Blecher-Prigat, A. 2011. "Privacy for Children." *Columbia Human Rights Law Review* 42. https://doi.org/10.1163/2210-7975_hrd-9947-0046.

Smirnova, S, Livingstone, S. and Stoilova, M. (2021) Understanding of User Needs and Problems: a rapid evidence review of age assurance and parental controls in everyday life. London: London School of Economics and Political Science (LSE).

Stoilova, M., Nandagiri, R., and Livingstone, S. 2021. "Children's Understanding of Personal Data and Privacy Online – a Systematic Evidence Mapping." *Information, Communication and Society* 24 (4): 557–75.

UNICEF. 2021. "Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper." https://www.unicef.org/media/97461/file/Digital%20Age%20Assurance%20Tools%20and%20Children%E2%80%99s%20Rights%20Online%20across%20the%20Globe.pdf.

UNICEF/Danish Institute for Human Rights. 2013. "Children's Rights in Impact Assessments, A Guide for Integrating Children's Rights into Impact Assessments and Taking Action for Children." https://www.unicef.ca/sites/default/files/2019-01/Childrens-Rights-in-Impact-Assessments.pdf.

Van der Maelen, C. 2019. "The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications." *Delphi* 3: 115–21.