code voor kinderrechten

Code for Children's Rights

The Code for Children's Rights was drawn up by
the University of Leiden and the Waag organisation and was commissioned by the
Ministry of the Interior and Kingdom Relations.

code voor
kinderrechten

Table of contents

The Code at a glance

Beginsel 1

Zet het belang van het kind voorop bij het ontwerp

Beginsel 2

Betrek kinderen en hun verwachtingen bij het ontwerp

Beginsel 3

Verwerk persoonsgegevens op een voor kinderen rechtmatige manier

Beginsel 4

Zorg voor transparantie op een voor kinderen begrijpelijke en toegankelijke manier

Beginsel 5

Voer een op kinderrechten gebaseerde privacy impact assessment uit

Beginsel 6

Zorg voor een kindvriendelijk privacy ontwerp

Beginsel 7

Voorkom het profileren van kinderen

Beginsel 8

Voorkom te allen tijde economische exploitatie van kinderen

Beginsel 9

Voorkom te allen tijde voor kinderen schadelijk ontwerp

Beginsel 10

Ontwikkel richtlijnen voor de branche die zijn gericht op de bescherming van de belangen en rechten van kinderen

The Code for Children's Rights helps developers and designers to focus on the rights of children when developing digital services. The Code consists of ten principles, presented on the basis of practical examples for implementation. The principles are not in themselves legally enforceable, but are based on law and regulations (such as the UN Convention on the Rights of the Child 1989) which are indeed legally binding.

Principle 1: Make the best interests of the child the primary consideration when designing. Prioritising the best interests of the child in all digital activities with an impact on children is the guiding principle throughout the entire Code. A digital service which might be used by children must take account of this principle and all other principles in this Code. A child impact assessment preceding the development and during the life cycle of the service can be used to carefully weigh up this principle against other interests. **Relevant laws and regulations**: Art. 3 UNCRC, Art. 24 (2) EU Charter of Fundamental Rights.

Principle 2: Involve children and their expectations in the design process. In order to realise the best interests of the child, children must be able to participate in some way in the design and development of digital services which have an impact on them. Make sure that you have an understanding of the target group (including their age category) which you wish to reach and create the design based on the group encountering the greatest number of limitations. Seek alignment with the perception of children and communicate in a manner which fits in with the relevant developmental stage. **Relevant laws and regulations**: Art. 12 UNCRC.

Principle 3: Ensure the legitimate processing of personal data of children. The personal data of children may only be processed in so far as this takes place in accordance with the law, whereby both general and child-specific rules apply. The principle of data minimisation is the primary principle of personal data processing. For the implementation, it is in some cases important to know a child's age category; it may be necessary to involve the parents of younger children. **Relevant laws and regulations**: Art. 16 UNCRC, Art. 8 (1) EU Charter, Art. 16(1) TFEU, and Art. 5 et seq. GDPR.

Principle 4: Provide transparency in a way that is understandable and accessible to children. Information on the use of a digital service must be recognisable and easy to understand for the child. In particular, the provider is obliged to provide transparency on the use and sharing of personal data. Make information on privacy accessible and understandable, and design tools within the digital service that allow children to be able to exercise their (data protection) rights. Take account of the child's age and stage of development. **Relevant laws and regulations**: Art. 3(1) UNCRC, Art. 5(1) GDPR and Arts. 6:230 m and 6:193c and d of the Dutch Civil Code (DCC).

Principle 5: Carry out a privacy impact assessment based on children's rights. Carry out a standard privacy impact assessment (PIA) based on children's rights whenever digital services might be used by children. As children are vulnerable users, the risk of breaching the data protection rights is high. Make regular use of the PIA to be able to keep properly assessing the

impact of the service. **Relevant laws and regulations**: Art. 16 UNCRC, Art. 8 ECHR, Arts. 7 and 8 EU Charter, Art. 35 GDPR.

Principle 6: Provide a child-friendly privacy design. Do not process more personal data than is strictly necessary for achieving the specific goal of the service. Include privacy in the design (privacy by design) and make the default settings as privacy-friendly as possible (privacy by default). Present this in a child-friendly form, e.g. with an 'opt-in' regime, standard, accessible built-in options to erase your data, and notifications when geolocation or microphone are on. **Relevant laws and regulations**: Art. 16 UNCRC, Arts. 7 and 8 EU Charter and Arts. 5 and 25 GDPR.

Principle 7: Prevent the profiling of children. Profiling users is a high risk form of data processing. A privacy-sensitive (and sometimes inaccurate) picture of an individual arises on the basis of correlations. Children are vulnerable as profiling can lead to stereotyping, stigma and discrimination. In addition, using profiling can encourage users to make excessive use of the service. Functions for profiling must be turned off as default, unless there is a compelling reason in the best interests of the child. In the latter case, appropriate safeguards should then be implemented. **Relevant laws and regulations**: Art. 2 UNCRC and Art. 22 GDPR.

Principle 8: Avoid the economic exploitation of children at all times. Avoid digital services geared to exploitation, such as encouraging in-app purchases, the use of gambling elements and personalised data-driven marketing. Be transparent about the commercial aspects of a service and avoid unfair commercial practices. **Relevant laws and regulations**: Arts. 3, 13, 32 UNCRC, Arts. 6, 7, 8, 21 and 22 GDPR, 6:193 DCC, Art. 3 Dutch Media Act and Art. 21 Dutch Betting and Gambling Act.

Principle 9: Avoid a harmful design for children at all times. A digital service can be harmful for children if the design abuses the vulnerability of children or does not adequately protect children against possible harmful content and behaviour. It is harmful if the (mental, social, cognitive or physical) development of the child is negatively affected, for example when resulting in them making excessive use of the service. It is therefore advisable to apply the precautionary principle ('better safe than sorry') if it is likely that a digital service is harmful even if conclusive evidence is still lacking. **Relevant laws and regulations**: Arts. 6, 17 and 24 UNCRC, Art. 5(1) GDPR and Art. 4 (1) Dutch Media Act.

Principle 10: Develop industry guidelines which are geared to protecting the interests and rights of children. The private sector plays an important role in the development and provision of digital services. Companies can themselves contribute to children's well-being by drawing up industry guidelines - preferably in consultation with children. **Relevant laws and regulations**: Art. 3 UNCRC, Arts. 5(2) and 40 GDPR and Art. 6: 193c (2) DCC.

Code for Children's Rights

Apps and games play an important role in children's lives. Children are also spending increasingly more time on apps and games.

Digital technology makes a valuable contribution to children's development. However practice has shown that in the design of technologies choices have been made which are not always in the best interests of the child.

The Code for Children's Rights consists of ten principles with practical examples which designers and developers can use to safeguard the fundamental rights of children in digital services.

Why a code for children's rights?

This code helps developers and designers to take account of children's rights when designing and developing apps, games, smart devices and other digital technology.

Children's rights must safeguard that children have sufficient freedom to develop and to participate in society (participation), while at the same time being protected against possible harmful influences, such as abuse and addiction. This participation is increasingly often taking place using digital services. It is therefore important that these services are designed in a child-friendly manner.

This Code provides tools and guidance which assist in the understanding of the rights of children and how to apply them in the development of a digital service. The principles are based on laws and regulations and all derive from the fundamental rights of children in the UN Convention on the Rights of the Child 1989 (UNCRC). Although the principles are in themselves not legally enforceable rules, the underlying laws and regulations are legally binding.

Who are we talking about when we say 'children'?

In the Code we speak of 'children', whereby we are referring to all persons under the age of 18 (Article 1 UNCRC). Sometimes the law refers to minors, but in such case we will still use the term 'children'. Sometimes the law mentions specific ages (e.g., Article 8 GDPR) and the rules in such a provision thus apply to that age group. Even if the group is not clearly defined on the basis of their age, according to the UNCRC account must be taken of the evolving capacities of the child (Article 5 UNCRC). When applying or implementing a rule it is possible that various ages must be taken into account, even if the law does not state such specifically.

To what digital technology does the Code apply?

The Code deals with the design and development of 'digital services'. This includes all services which in some way make use of digital technology, including apps, games, websites, devices connected to the network (including toys and smart assistants), online platforms, etc. This concerns all digital services that children might use, even if they are not explicitly geared to children.

To whom is the Code directed?

This Code is, in the first place, directed at businesses, governments, organisations and independent parties who design and develop digital services. Designers and developers will be given concrete tools and guidance to ensure observance of children's rights in the designing and developing of services.

The Code is also relevant to other parties, such as a client and a brand holder. The design of a digital service requires commercial decisions of, e.g., a director or investor, which have consequences for the design. It is equally practical for company lawyers and data protection officers in an organisation to take note of specific rules for children. The Code also has an added value for digital platforms or app stores which provide software of third parties and want to know what standards based on children's rights any apps must satisfy. In addition, the Code is relevant for organisations which use software for or with children and want to know what they should specifically look out for upon acquisition and use, for example, public authorities, schools or youth care organisations. Lastly, the Code – and in particular principle 10 – is directed at industry organisations with the request to develop codes of practice based on children's rights.

The Code is ultimately intended for anyone who uses digital technology, including of course children and parents, or who is responsible for the implementation of children's rights in policy and regulations.

How did we establish this Code?

The first two principles are overarching principles which follow directly from two of the four fundamental principles of the UN Convention on the Rights of the Child 1989 (UNCRC): the interests of the child and the right of the child to be heard. These rights have an effect within the other principles. The other principles are also based on the rights in the UNCRC and other laws and regulations.

The Code is limited to those laws and regulations, and in particular to the provisions laid down therein in which children *in particular* are protected (e.g. provisions relating to the processing of personal data, unfair commercial practices or harmful content) or in which the interests of the child were included in the interpretation of the rules.

The principles in this Code are interconnected and are in their entirety relevant for the design and development of digital services which are used by children. It is thus not a 'pick-and-choose' model whereby only a few, random principles are implemented. The concrete implementation is dependent on the specific goal and intended design of an app or game. Where possible we will refer to best practices for the implementation.

The Code has been drawn up in consultation with experts in the intersection of the child and technology, and with designers, developers and young people.

Terminology

The Code speaks of the 'user' (e.g. the child and/or the parent) and the 'provider' of a digital service (the business that designs, develops and/or provides the digital service). We also use these terms in places where the legislation uses more specific terms. For example, terms like 'data subject' or 'data controller' in the data protection legislation or 'consumer' and 'business' in consumer law. Legislation sometimes refers to 'information society services', by which it means commercial digital services. In addition, the term 'parents' also includes other legal guardians or carers of a child.

Principle 1: Make the best interests of the child the primary consideration when designing

Explanation

The interests of the child must be a primary consideration in all digital activities with an impact on individual children, groups of children, or children in general. When interpreting all principles in the Code – and consequently all aspects of the design – the interests of the child are the guiding principle. The principle seeks to contribute to the full and effective safeguarding of the fundamental rights of the child. The interests of the child do not stand alone, but must be seen in the light of all relevant rights of the child in a specific situation. In the broadest sense, the interests of the child entail that activities which have an impact on children must safeguard the well-being and the development of the child.

Digital technology can make an important contribution to the development of a child, e.g. by the facilitation of social interaction or the stimulating of creativity. However practice teaches that, in the design of technologies, choices are often made which are not in the interests of the child and which may indeed be harmful to them. It is therefore not sufficient to only prevent harm or negative consequences for children. The interests of the child also mean that the child must be able to have an equally 'rich' online experience as an adult. Children may not be simply excluded or deprived of specific experiences.

The interests of the child is a continual point for attention in the design and use of a digital service, from the time that a start is made in the realisation of the idea and during the entire life cycle of the digital service.

Implementation

Assume that a digital service which might be used by children must take account of the interests of the child and all other principles in this code. It must also be assumed that – regardless of a minimum age which is stated in the terms of use – measures must be taken to safeguard their interests even if there is no adequate age verification.

Prior to the design of digital services, you must chart the interests of children and weigh them up against other interests, including interests of other children, parents and businesses themselves. The interests of the child must also be a primary consideration with regard to the commercial interest that a business has in providing a digital service. This does not mean that a digital service may not pursue a commercial interest, but in the weighing up of the interests it is

explicitly stated that the interests of the child are a primary consideration. When weighing up the interests, account should be taken of the various stages of development of children on the basis of their age and social, mental and cognitive development. The weighing of interests and the implementation of the 'interests of the child' principle prior to the development of a digital service consists of two stages. We call this exercise a child impact assessment[1]. A team of interested parties and experts are involved in the child impact assessment to provide input on decisions on all kinds of aspects of the service, for example designers, developers, investors, privacy officers, marketeers, (company) lawyers and, where possible, children themselves.

Stage 1: assessment stage

In this stage *all* factors which are relevant in the light of the interests of the child have been charted and assessed. In this respect account is taken of the child's age[2] (see also the page more information[3] on the development stages of a child or principle 3 for ways to check a user's age).

Relevant factors are, inter alia:

a. possible impact on the well-being and the development of children;
b. possible impact on the rights of children. This includes the following rights:
    - right to non-discrimination,
    - right to freedom of information,
    - right to freedom of opinion and thought,
    - freedom of association and identity forming and
    - right to play and engage in recreational activities;
c. possible impact on the safety of children. For example:
    - guaranteeing privacy (including the confidentiality and integrity of personal data and the identity of children),
    - protection against all forms of exploitation, including commercial or sexual exploitation and sexual abuse,
    - protection against social risks, including digital bullying and
    - preventing confrontation with harmful information;
d. the role of parents in safeguarding the interests of the child, including in providing protection from potential risks and in supporting safe and fruitful use of the digital service.

---

[1] https://sites.unicef.org/csr/css/Children_s_Rights_in_Impact_Assessments_Web_161213.pdf
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/?q=participation
[3] https://codevoorkinderrechten.nl/meer-informatie/

In so far as available, the assessment of the factors will be supported by scientific research. In addition, expectations, insights and views of children must be included in the assessment where possible (see principle 2).

Stage 2: determination stage

On the basis of the assessment in stage 1, it is concretely determined what organisational and technical measures are necessary to adequately safeguard the interests of the child (and thus children's rights) in the design and subsequent use of the digital service. The following questions provide guidance:

a. What specific safeguards are required by laws and regulations with an eye on the best interests of the child?
b. What design choices are most in the best interests of the child? Make use of the results of the assessment stage.

The second stage is an accountability stage in which the parties in question concretely show how the interests of the child are implemented in the digital service.

The manipulation of children (including in the exercising of their rights) in a manner which only, or primarily, serves the commercial interest, is not permitted (see principle 8). Focusing on a commercial interest with a digital service is permitted, as long as it can be demonstrated that the best interests of the child are a primary consideration when a digital service has, or might have, an impact on children. The provider will thus have to be able to demonstrate that it has taken account of the best interests of the child in a child impact assessment as set out above.

A child impact assessment (consisting of stage 1 and stage 2) is not a one-off exercise, but must be continually updated. The concrete use, and the further development of, the digital service can give rise to an adjustment of the concrete measures or design choices in the best interests of the child. Sometimes the impact which an app or game has on children only becomes clear by how their users interact with it. Think of apps like Pokémon Go whereby children come into physical contact with users of a variety of ages. With every innovated application or update of the digital service, you must again ask the question whether the best interests of the child are paramount.

Relevant laws and regulations

Children's rights perspective

The obligation to take account of the best interests of the child in all activities which have an impact on children can be found in Article 3(1) of the UN Convention on the Rights of the Child[4] and Article 24(2) of the EU Charter of Fundamental Rights[5]. The implementation of the best interests of the child requires a specification of all relevant children's rights in the design of a digital service with an impact on children. Relevant children's rights can be: right to freedom of information, right to access to (non-harmful) media, right to freedom of opinion and thought, right to freedom of association, right to privacy and data protection, right to identity development, play and leisure, right to protection from violence (including bullying and sexual abuse) and from economic exploitation.

In the implementation of relevant children's rights a balance must be found between the data protection rights of children and their other rights, including their rights to development (Article 6 UNCRC), freedom of expression and freedom to seek, receive and impart information (Article 13 UNCRC) and association and assembly (Article 15 UNCRC). In addition, you must take account of the age of children and their evolving capacities (Article 5 UNCRC). Some design choices can be in the best interests of a 16-year old, but not in the best interests of a 6-year old. For younger children it can be justified to place greater emphasis on their rights to be protected, while for older children the freedom rights can be deemed more important. Special attention must be given to making digital services accessible to children with a physical limitation.

Children themselves find it important that providers of digital services, in their interests, better comply with the rights which children have on the basis of the UN Convention on the Rights of the Child 1989. According to the UN Committee on the Rights of the Child, public authorities must see to it that providers prevent that the safety and well-being of children comes under pressure from the use of digital services. Providers must carry out thorough research into the impact of their products and services on children and must publish their underlying child impact assessment.

---

[4] https://wetten.overheid.nl/BWBV0002508/
[5] https://wetten.overheid.nl/BWBV0002508/

Data protection legislation

The General Data Protection Regulation[6] (GDPR) seeks, among other things, to contribute to the "well-being of natural persons" (recital 2). However, the interests of the child are most clearly expressed in recital 38, which states that children enjoy specific protection in the light of their fundamental right to data protection: "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data".

Other considerations in the GDPR 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 is risky). These recitals were elaborated in the provisions of the GDPR.

Aside from the fact as to whether children are mentioned explicitly in recitals or provisions of the GDPR, when it comes to data processing which has an impact on children, account must always be taken of the best interests of the child. The 'best interests of the child' principle and the GDPR apply in all following principles in this Code.

Consumer legislation

Children are not always specifically mentioned in consumer legislation, but the 'best interests of the child' principle requires, in the case of a (presumed) impact on children, that consumer legislation is interpreted in such way that the development and the well-being of children must be taken into account.

An exception in consumer legislation where explicit account has been taken of children is in the regulation of unfair commercial practices (6:193a Dutch Civil Code (DCC) et seq.) (see principle 8). This legislation protects the average consumer against commercial practices which disrupt his or her economic behaviour by, e.g., being misleading or by exerting pressure. The degree of influence can be measured by taking a fictitious average consumer as the starting point. If a commercial practice is geared to a specific group of consumers, like children, the effect of the practice is assessed from the perspective of the average member of the group in question (Article 6:193a(2) DCC). Children can in this context be deemed particularly vulnerable, in view of their age and their specific development (Article 5 UNCRC). If an app or game is therefore geared to children, the average child in the relevant age group is the yardstick for the degree of protection.

---

[6] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679

In addition, the provider must take account of the average member of the group for which it can be reasonably foreseen that he or she will be particularly susceptible to the commercial practice or the underlying product. In order to determine whether a digital service must indeed take account of children (of a specific age), it must be reviewed to what extent the provider could reasonably have expected that this practice would (in particular) appeal to vulnerable groups or that these groups, because of their vulnerability, including their mental or physical disability, age or gullibility, are particularly susceptible to the practice.

Other legislation

Harmful audio-visual content - The Dutch Media Act 2008 protects children from confrontation with harmful audio-visual content via, e.g., video on demand services. Since 2020, video platforms or social media which are used to share videos must protect children from harmful content, the incitement of hatred and violence, and advertising (see principle 9).

Principle 2: Involve children and their expectations in the design process

Explanation

Children must be heard or be able to participate in some way in the development of digital services (which can have an impact on them) in order to help flesh out the interests of the child. Digital services will have that impact if it is likely that they are actually used by children. Children are creative and have a lot of ideas which can be of value for the design of a digital service. By involving children you can better align with their perspective of the world and gain insight into what obstacles they experience in the use of an app.

In order to let children participate in the design process, it is important to understand what possibilities there are, depending on the age of the child. This requires special knowledge as well as experience in working with children. The participation of children goes further than the execution of a user test. It also encompasses the question as to whether a digital service can make a contribution to the mental, social and cognitive development of the child, including in the longer term. Naturally you must also take account of social and cultural factors. You must also not forget to involve children who have special wishes and needs because of, e.g., a disability or because they have access to digital technology to a lesser degree. Actual participation by children in the design process requires that children be properly informed about the idea and the choices that exist.

The involvement of children also has a procedural side. This entails that children must be given the opportunity to report questionable matters which arise when using the app. Here too account must be taken of the child's age. For example: what is offensive for children of what age and at what age are they able to independently safeguard their interests?

Youths (14-16 years old) who are involved during the drawing up of this code have confirmed that they enjoy joining in the process. On the basis of their own experience, they have all kinds of concrete ideas about what a service should look like. As one of them said: "I like that we're finally being asked what we think about this." Their remarks will be mentioned in the Code by way of illustration.

Implementation

Involve children in the design stage from the start. Make sure that you have an understanding of the target group which you wish to appeal to and intend to involve in the design. Take the child who has the most limitations in the selected target group as the starting point. In addition, try to design various characters and to avoid stereotypes (like gender roles), and give children the possibility to accept various characters and roles.

Make use of the Web Content Accessibility Guidelines (WCAG[7]) to make the service accessible to children with a disability, like impaired vision, deafness and impaired hearing.

There are many examples for involving children in the design and the development of services. Some important advice of designers and developers for the joint design process is shown below:

- Put children at ease. Children must feel safe and have the idea that they are being listened to. You can do this by, during the session, placing emphasis on the good in people and telling stories about negative emotions or experiences in the first person. In your communication focus on the strong points and potential of the child.
- Choose your words carefully when explaining an assignment, do not use trade jargon, like the language of a designer. Seek alignment with children's vocabulary and daily lives. Children like to receive explanations about digital technologies from people in their direct environment, like teachers, a principal or a parent.
- Be specific, for example about the most common or most recent apps, or about screen time.
- Give as few hints as possible. The insights of children are more valuable when you let children speak freely.
- First ask children whether their experience was good, so-so or bad. Providing such a choice of answers helps children get going when it comes to sharing their experience. Using this classification, keep asking the child questions.
- Test every stage with a different group of children (involving the same group of children can lead to false positive results).

[7] https://wcag.nl/

The UNICEF guidelines[8] and the recently published British Age Appropriate Design Code[9] with guidelines for communicating with children can be of use here.

Involving children is not only relevant during the design stage prior to building an application, but is an iterative process (as has also been mentioned under principle 1). During the development of all subsequent updates and modifications it is useful to actively involve children, whereby you can include complaints and feedback from user experiences. It is therefore recommended to build in a feedback mechanism for after the design stage of a service.

If you are going to involve children in your design, you can, for example, consult the Digiraad[10] and the 'child ministers of Digital Affairs' who are already participating in an organised manner in coming up with ways to involve children's rights in the design of digital services.

Relevant laws and regulations

Children's rights perspective

The right of children to be heard (Article 12 UNCRC) is one of the fundamental principles of the UNCRC. The principle is integrally connected with the best interests of the child (Article 3(1) UNCRC) (see principle 1). In order to be able to implement the best interests of the child in activities which have an impact on children, it is necessary to know what children's expectations, concerns, wishes and needs are. In order to determine these, children must be involved in some way. Account must be taken in this respect of the development of children (Article 5 UNCRC): as of the age that they are able to have and share insights, this right must be respected. The right of children to be heard is furthermore also connected with all other rights of the children in the UNCRC. For example, the right to development (Article 6 UNCRC), the freedom of expression and information (Articles 13 and 17 UNCRC) and the freedom of

[8] https://sites.unicef.org/cwc/files/CwC_Final_Nov-2011.pdf
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/
[10] https://saferinternetcentre.nl/digiraad/

association (Article 15 UNCRC). The right to be heard contributes to respect for human dignity and a healthy development of children.

The Council of Europe indicates in the Guidelines to respect, protect and fulfil the rights of the child in the digital environment,[11] that the right of children to be heard entails that the right of children to safe participation relates to digital technology. In particular, the Council expects that "States and other relevant stakeholders (...] actively engage children to participate meaningfully in devising, implementing and evaluating ... technologies and resources that aim to respect, protect and fulfil the rights of the child in the digital environment"[12].

The UN Committee on the Rights of the Child acknowledges that the government must ensure "that digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services." (General Comment 25). In order to be heard, the Council of Europe also believes it is important that children are informed "of restrictions in place, such as content filtering, in a manner appropriate to their evolving capacities, and that they are provided with guidance on appropriate remedies, including on how and to whom to make a complaint, report an abuse or request help and counselling. Where appropriate, parents or carers should also be informed of such restrictions and appropriate remedies"[13].

When involving children, account must also be taken of children in deprived or vulnerable circumstances, as well as of children who have suffered harm in some way from the use of digital services.

Data protection legislation

Children can also be involved in the protection of their personal data through the data protection legislation.

By means of a Privacy Impact Assessment (PIA) (Article 35 GDPR) (see principle 5), children and their parents can be given the opportunity to have a say in the way in which their data are used. This can be beneficial for confidence in the digital service. It also helps to understand

---

11 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046c478

12 https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

13 https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

what wishes, needs and concerns they have with regard to the digital service and in particular the way in which personal data are used.

In addition, it is also important to have insight into the privacy expectations of children if legitimate interest in Article 6(1)(f) GDPR is the legal basis for processing their personal data (see principle 3). With said legal basis there is a weighing of interests, whereby you only have a legitimate interest if your interest is more important than that of the person whose data you are processing. You can only know the best interests of the child if children are heard in some way (see principle 1). But in particular it is a requirement under this provision that you take account of the reasonable expectations of the person whose personal data you are processing.

It is furthermore important to involve children in finding the way most suitable and recognisable for them to provide information on the processing of personal data (see principle 4). This must take place in a way which is concise, transparent, comprehensible, in an easily accessible form and clear and easy language, where in particular attention is paid to what is appropriate for children (Article 12 GDPR). Being adequately informed is also a prerequisite for the validity of consent (Article 7 (2) GDPR) as a legal basis (Article 6 (1) (a) GDPR), for the processing of personal data (see principle 3), and to be able to know what works with children, you will have to engage them.

Lastly, the GDPR considers in the framework of codes of practice (see principle 10) that "When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of [providers] should *consult relevant stakeholders, including [users] where feasible, and have regard to submissions received and views expressed in response to such consultations* (recital 99). In addition, the European Data Protection Board indicated in its guidelines that a consultation in sectors with a high risk, including those where the data of children are processed, may be more extensive.

Principle 3: Ensure the legitimate processing of personal data of children

Explanation

The personal data of children may only be processed as long as the processing is in accordance with the law. In addition to the general rules which apply regardless of the user's age, the law includes rules which offer specific protection to children. This not only applies to the data protection legislation, but also to consumer legislation. These specific protection rules exist because children can be extra vulnerable. For example, because they understand less well what takes place with personal data within the inner workings of an app or game or because they can be more easily influenced by making choices in digital services.

In order to properly apply the special rules geared to children, it is necessary to know which of the users is younger than 18. And in order to implement those rules in a manner appropriate for the - possibly different - ages of the underage users, it is important to know what age category a child falls under. Younger children may require a different implementation of the rules than older children. For example, in the first case it might be necessary to involve the parents in decisions or to have certain choices restricted as the default setting.

Implementation

Apply the principle of data minimisation: process the fewest possible data of the child.

- Determine for each separate part of your service what personal data you need to be able to offer them.
- Determine separately for each individual component of your service what personal data you need and for how long you need them to be able to offer the relevant component. In principle, ask for and process only the absolutely necessary data. Where possible, give the child the choice as to what components of your service they want to use.
- Only collect the personal data if the child is actively and consciously using that relevant component of your service. For each additional purpose, the choice must be presented to the user if the legal basis is consent.

- The collecting of personal data to personalise, improve, optimise (etc.) the online experience of your users outside of the core service may not be simply combined with the personal data which you use for the core service.
- Do not exclude specific services for users who opt not to share a part of their data, for example by not requiring a personal profile picture or exact geolocation (unless necessary for the functioning of the service and then possibly limited to a specific user session).
- Exercise restraint in the use of web forms. Only request data which are necessary for the use of a service. Where possible, anonymise these data, or apply 'datafading' (anonymise data gradually: anonymise data after processing). Another option is pseudonymisation; there are several options for protecting the personal data of the users with technical and organisational measures.
- Encourage the use of adblockers, like Junkbuster, CookieCooker or the Firefox Add-on, or Self-Destructing Cookies, so that cookies are immediately removed when a webpage is closed. See for more design solutions geared to, among other things, minimal data processing[14].**

In line with the principle of data minimisation, it is advisable to consider whether it is relevant to verify the age (category) of your users, certainly when it comes to services which do not entail any risks (for example, according to the child impact assessment of principle 1 or the privacy impact assessment of principle 5). If the use of the service does entail risks, where necessary take account of the possible age of your users. Take the youngest age category as the starting point (see for the categories the table in the annex). The table on age categories which use the Age Appropriate Design Code (to be viewed in the downloadable PDF or via this link) can help in this respect.

There are various ways to verify the user's age category. By verification we mean that you determine whether a child is younger than a specific age (e.g. 16 or 18) or falls in a specific age range (e.g. 12-15 years of age) without your having to know precisely how old the child is. Examples of ways to verify age are:

- User statement. Ask the user whether he or she is younger than a specific age or is in a specific age group, without their presenting any proof. This form of age verification is appropriate for the processing of low risk data or can be used in combination with another (for example the following) verification technique. Bear in mind that this form of age verification is probably not adequate when processing personal data of children.

[14] https://privacypatterns.org

- Technical measures. In order to discourage users from making incorrect age statements and/or to track incorrect statements down and to make the opening of accounts by minors impossible, such as with digital services which can be harmful for children (for example gambling or porno sites), technical measures are an option. Think of a neutral presentation of the windows in which users must indicate the age category they fall in (and consequently do not encourage them to choose another age category), or which, for example, bring about that users cannot immediately specify another age category when it turns out that with the earlier specified age category they cannot gain access to the service. When it comes to 18+ websites, it is strongly advised to discourage users from giving an incorrect age using the same technical and organisational measures.
- Third parties. You can also outsource the age check to a third party. These kinds of services work with attributes ('Attribute-Based Credentials'): you ask for confirmation of a specific user attribute (in this case the age category) and the service answers 'yes' or 'no'. Naturally this service must satisfy the requirements for data protection and you must provide users with clear information on the fact that you are making use of this service. Such a verification will preferably take place on the user's device. The third party only facilitates the age verification but will not process any personal data. One example of such a service is IRMA[15].
- Confirmation via e-mail or text link. For example, ask the parent to confirm the child's age by clicking on a link which is provided in an e-mail or a text message.

Make sure that the data which are collected are not used for purposes other than age verification and do not process any more data than is absolutely necessary. Only apply the other principles in this code to the lowest identified age category (highest protection level).

Take a LIA (Legitimate Interests Assessment) when you want to collect data on the basis of 'legitimate interest'. A LIA is a more simple form of risk assessment (than a PIA) which pushes you to determine the goal of processing and to think about the consequences for persons[16]. A LIA can be a reason to carry out a (more in-depth) PIA (see principle 5) but assume that a PIA is in any event necessary if a service is probably used by children.

Only furnish data to third parties or to other departments within your organisation if there is a demonstrable compelling reason for this (such as legislation), taking account of the best interests of the child. Commercial reuse of personal data is (probably) not a demonstrable

[15] https://privacybydesign.foundation/irma/
[16] For an example: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

compelling reason. Use the PIA for this (principle 5) and study the problems and risks which arise from the PIA. Make sure that you have a guarantee from the third party that it will not use the personal data in a manner which is harmful to the well-being of the child.

Make it just as easy for children to cancel a digital service as it is to register for it. Make sure that personal data which are no longer necessary are deleted.

Relevant laws and regulations

Children's rights perspective

The UN Committee on the Rights of the Child indicated that the UNCRC, in particular Article 16 on the right to privacy, encompasses a child's right to data protection. European citizens, including children, have a fundamental right to data protection (Article 8 (1) Charter of Fundamental Rights of the European Union (EU Charter), Article 16 (1) Treaty on the Functioning of the European Union).

The fundamental right to data protection has been realised in the European Union in the General Data Protection Regulation (GDPR): "The protection of natural persons in relation to the processing of personal data is a fundamental right" (recital 1 GDPR) and the GDPR "respects all fundamental rights and observes the freedoms and principles [...], 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" (recital 4 GDPR). "All fundamental rights" also encompasses the rights of children and in particular the best interests of the child (Article 3 UNCRC, Article 24 EU Charter) (see principle 1) and the right of children to be heard (Article 12 UNCRC) (see principle 2) .

The GDPR explicitly acknowledges that the children's rights perspective is important: "[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" (recital 38 GDPR).

Data protection legislation

The basic principles of the data protection legislation

Providers of digital services which process personal data must satisfy the rules of the GDPR. If their services have an impact on children then there are special points of attention for the

protection of the personal data of children under the GDPR. This starts when applying the seven basic principles of the data protection legislation. These are the principles of lawfulness and fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability (Article 5 (1) (a) - (f) GDPR). The basic principles of data protection in Article 5 of the GDPR are very important because they form the basis (hence 'basic principles') of the rights and obligations in the GDPR. In addition, any breach of these principles can lead to higher fines than when there is action in contravention of some of the obligations in the GDPR (Article 83 (5) (a) GDPR).

These basic principles can set higher requirements for the data processing relating to children, e.g. because account must explicitly be taken of the best interests of the child (see principle 1). For example, when applying the lawfulness and fairness principle, it is relevant whether there is an unequal power relationship between the provider of a digital service and the user. Due to their vulnerable position, when it comes to children there will more quickly be an imbalance or a greater imbalance than in the case of adults. A child's age may also play a role in the question as to the degree of imbalance in the power relationship between the child and the provider. Furthermore, the duty of accountability - i.e. the obligation to demonstrate that a business satisfies the GDPR (Article 5 (2) GDPR) - may have a more substantial elaboration for children due to their vulnerable position and have a special need for protection.

When it comes to children, the fleshing out of the principle of legitimacy of the processing of personal data also calls for special attention. The principle requires that the processing is legitimate (Article 5 (1) (a) GDPR) and the processing of personal data is not legitimate if it is not based on one of the six legal bases stated in Article 6 of the GDPR: consent, contract, compliance with a legal obligation, public interest, vital interests of the data subject or legitimate interests of the data controller (Article 6 (1) (a)-(f) GDPR).

Legal bases

Personal data may only be processed if there is a legal basis for the processing. The legal bases are exhaustively listed in Article 6 (1) (a)-(f) of the GDPR. In order to be able to determine what the most appropriate basis is from the perspective of lawfulness and fairness, you will first have to determine the specific purpose for which the data are being processed. Every specific purpose requires a separate legal basis. Below the focus will be on three of these bases: 'consent', 'necessary for the performance of a contract' and 'legitimate interest'.

Consent (Article 6(1)(a) GDPR, Article 7 GDPR, Article 8 GDPR))

The processing of personal data can be legitimate if the user has given consent for one or more specific purposes. The user must give valid consent by means of a clear active action (written / verbal statement, including by electronic means), from which it appears that they accept the relevant processing of personal data freely, specifically, informed and unequivocally (Article 7

GDPR). For digital services which are used by children, it will in particular have to be studied whether the conditions for consent have been satisfied. For example, has a more appropriate way been chosen for children to inform them of the data processing (informed consent) (see principle 4)? Has the consent been given freely, in view of the fact that the power relationship between children and a provider of digital services is possibly more lop-sided (free consent)? Consent is not freely given if there is no true choice. The reason can be contextual (for example, data processing which is mandatory for the citizen or student by the government or in education) or there are economic considerations (such as earnings models based on data-driven marketing whereby personal data is used as "payment" for using the digital service (see Article 7 (4) GDPR) (see principle 8). True choice is lacking, e.g. if the use of a service is dependent on privacy conditions relating to processing which is not strictly necessary. In all those kinds of cases - consent is not a free choice – consent cannot be the legal basis and another appropriate basis will have to be found in Article 6 GDPR.

Specific consent means that there must be agreement to the processing of a specific kind, a specific activity. The consent which is given must apply to all processing activities which serve the same purpose. If there are several purposes for the processing, an individual must agree to each of these purposes separately or another legal basis must apply. The consent must also be unequivocal, which entails that what the individual is agreeing to must be clear; the text with which the person agrees must be open to only one interpretation. This condition entails that, for example, the use of pre-ticked boxes or inactivity may not be deemed consent. An individual who has consented to data processing must be able to withdraw that consent just as easily (Article 7 (3) GDPR). The digital services provider must be able to show that the consent has been validly given by the user (duty of accountability, Article 5 (2) GDPR).

When consent is the legal basis, children of 16 and older can give consent themselves (Article 8 GDPR in conjunction with Article 5 of the Dutch GDPR Implementation Act). Be aware: other EU Member States may apply different ages (15, 14 or 13 and older) and in the United States the age is fixed at 13 and older. The safest option is to only ask children of 16 or older independently for consent because this is always okay (provided the other conditions for lawful consent are met). The processing of personal data of a child younger than 16 is only valid if the consent is granted by the person who has parental authority for the child. This will often be one of the parents, but it can also be another legal guardian. Be aware that this age limit applies in the Netherlands; in other countries of the European Union another age limit may have been chosen.

In order to be able to apply these rules, you have to know when you are dealing with someone who is younger than 16. There is an implicit obligation to determine this. The rules for this are strict, because only if a digital service is offered to customers who are older than 18 and there is no proof of the contrary, for example, it is not the case that children will in fact use it due to flawed age verification, may it be assumed that the digital service is not provided to children. In that case you do not have to check whether children are older or younger than 16. In the event

that a child is younger than 16, not only will parental consent have to be requested, it will also have to be verified that it is indeed the parent (or other legal guardian) who gave consent for the data processing.

Reasonable efforts must be made to verify through means that satisfy the state of the art. When building in age verification and verification of parental consent, no more personal data may be processed than is strictly necessary (principle of minimum data processing or data minimisation) (see principle 6). Parental consent is not required for preventive and advisory services to children (recital 38). Think of the Kindertelefoon (children's helpline) where children can chat confidentially about any problems they are struggling with. Whether it is the children or the parents who may or must give consent, the previously mentioned requirements for consent must always have been satisfied. Bear in mind that when a child turns 16, consent can be requested again, but this time from the child themself. In addition, children can have an interest in withdrawing consent and having data erased when they turn 16 and may themselves decide on the processing of their personal data. These options will thus have to be built in, in a manner which is accessible and understandable to children.

Contrary to what is sometimes believed, consent is not necessary for legitimate data processing if there is a different legal basis. Digital services often make use of the legal bases of contract (Article 6 (1) (b) GDPR) and legitimate interests (Article 6 (1) (f) GDPR). In view of the stringent conditions for consent as legal basis, which are even more stringent for children, consent may not be the most desirable basis for providers of digital services.

Necessary for the performance of the contract (Article 6(1)(b) GDPR)

Data processing is also legitimate if it is *necessary* for the performance of a contract with the user of the digital service. This is one of the legal bases which is often used with digital services. The digital service provider must be able to show that there is a contract, that this contract is valid, and that the processing of personal data is also *actually necessary* for the *performance* of the contract (duty of accountability, Article 5 (2) GDPR).

This legal basis has another complication with regard to children because, on the basis of the applicable law, children must be able to validly conclude a contract. Whether processing is necessary depends on the specific purpose for which the data are processed and, partly in the light of the best interests of the child (see principle 1), account will have to be taken of the principle of minimal data processing (see principle 6) and the lawfulness and fairness principle (Article 5 (1) (a) and (c) GDPR). This does not include data processing intended for, e.g., data-driven and targeted marketing or the improving of an app or website. The drawing up of user and personality profiles or the monitoring of the behaviour of users to combat fraud cannot take place on the basis of this legal basis.

Legitimate interest (Article 6(1)(f) GDPR)

Another legal basis which is often used with digital services is the one whereby data may be processed if this is necessary for the benefit of a legitimate interest of the provider of such a service or a third party (Article 6(1)(f) GDPR). Legitimate interests can be, for example: combating fraud, marketing, technical security and counteracting illegal activities. Some legitimate interests can carry greater weight than others.

This principle asks for a weighing of interests between the legitimate interests of companies and the interests and rights of the users of the service, including children. This weighing of interests, in particular the best interests of the child (Article 3 (1) UNCRC) (see principle 1) and the fundamental rights of children in, inter alia, the UNCRC are considered. In particular the right to privacy and data protection of children must be included in the weighing of interests, but other fundamental (children's) rights, including the right to freedom of information, the right to access to media and the right to development, can also be relevant.

The application of this legal basis comprises three steps:

1. Determining of the legitimate interests of the provider of a digital service and consequently the purpose of the processing;
2. Showing why it is necessary to process personal data for the specific purpose that has been determined;
3. Weighing the necessary legitimate interests against the interests and fundamental rights of the user of a digital service.

Account must be taken of the impact which the data processing has on children (see principle 1) and what expectations children may reasonably have about the way in which their personal data are used (see principle 2). If marketing is presented as a legitimate interest, then in particular, e.g., account must be taken of the possible harmful impact of marketing on children. With data-driven forms of marketing, including the drawing up of user profiles, online direct marketing and online behaviour-steered marketing, the legal basis of consent (Article 6 (1) (a) GDPR) is deemed more appropriate. In the case of direct marketing, the user of a digital service has the right to object and will have to be informed about this in an accessible and proper manner whereby account must be taken of what children can understand at different ages. This only applies in the event that the application of this legal basis for direct marketing with children is legitimate, because it is not at odds with their interests and rights.

The digital service provider must see to adequate safeguards to limit unnecessary, and for children, negative consequences. This can include such things as 'privacy by design' solutions (see principle 6) and extra attention for transparency (see principle 4). The provider must be able to show that the best interests of children were a primary consideration in the weighing of interests and that it took account of the protection of the rights of children who are influenced

by the use of the service, in particular the data processing necessary on the basis of the provider's legitimate interest (duty of accountability, Article 5 (2) GDPR). The privacy conditions must explain what are legitimate interests (see principle 4). If a service is not specifically intended for children, the provider will have to check whether it is likely that children will use them.

Special categories of personal data

If there is processing of special categories of personal data, then in addition to the legal basis of Article 6 of the GDPR, the special and more stringent rules in Article 9 GDPR and Article 22 in conjunction with Art 23 Dutch GDPR Implementation Act must be satisfied. This concerns data about, among other things, a person's sexuality, ethnicity or health. It also covers biometric data. The processing of these personal data is not permitted, unless one of the ten legal processing grounds applies (Article 9 (2) GDPR).

One of those processing grounds is explicit consent. Explicit relates to the way in which the consent is expressed. An explicit way to give consent is to sign a written statement and this is possible by means of an electronic form or an email. The consent must be explicit to prevent that in the future there is doubt and/or lack of proof as to the existence of consent for these kinds of data processing. Because of the explicit character, the explicit consent is thus more stringent than the consent of Article 6(1)(a) GDPR. Furthermore, this form of consent is subject to the previously discussed conditions (Article 7 GDPR) for consent whereby there are special rules in the case of children younger than 16 (Article 8 GDPR).

Principle 4: Provide transparency in a way that is understandable and accessible to children

Explanation

Legal obligations in the data protection legislation and the consumer legislation stipulate that a digital provider must be transparent for users in various ways. A primary reason for this is to safeguard confidence in a digital service. Transparency is in fact a fundamental principle of data protection law and is therefore of great importance. As a digital provider, you must clearly indicate for what (legitimate) purpose you use what personal data and with whom you share them. You must also indicate for every purpose on what ground the processing is based and inform your users as to their rights.

With children there is the extra obligation to provide all that information in a manner which is recognisable, accessible and understandable to children. Because children are seen as a vulnerable group in data protection law, digital service providers have an extra responsibility to ensure that they properly perform this obligation, precisely for their benefit. It is therefore important to take account of the child's age.

Consumer protection law requires transparency regarding all aspects of a transaction. This means, for example, that a digital service provider must be clear about the costs in apps or games for, e.g., extra functionalities, lives or virtual goods (things like 'skins') which are purchased. It must also be clear for children that these purchases are for real money. This is particularly relevant when a game has its own currency (for example, V-Bucks in Fortnite). This obfuscates the link between real money and the purchase even more, certainly for children. Within consumer protection law, providers sometimes have a greater duty of care with regard to children, because they are seen as extra vulnerable consumers.

Transparency is a continuing responsibility of providers which must be guaranteed, not only when users are registering with a digital service, but also during the use thereof. Even if parents are involved in some way (e.g. because they must give consent for the data processing), the provider is nevertheless responsible for providing transparency geared to children and they must see to it that children understand what will be done with their data and what impact this has. This is not always easy to explain. It may be easier to make someone aware of social privacy risks, e.g. in dealing with parents or peers, than of the impact of processing personal data by digital service providers which is usually not immediately visible.

Young people do indeed see the risks in data processing, as appears from a remark in one of the sessions which we organised for drawing up this code: "**An app is harmful if they store my private data and do not erase them when I no longer have the account or if they pass my data on to other people**". At the same time, virtually no one reads the privacy terms; young people found them a **"really long story filled with technical talk**" and "**often hard to understand**". They should be presented in a more accessible manner.

Implementation

Make sure information on privacy is clearly visible to (underage) users.

- Add a privacy dashboard that children can understand, so that you can see at a glance what has been agreed.
- Make sure that the terms are concise, prominently displayed and clearly formulated in language that is easy to understand.
- Compel full reading of the terms as much as possible, e.g. by having the user agree to each section individually.
- To make it easier for users to follow the privacy settings, it is recommended to make use of visual elements which determine the level of privacy. For example, make use of (drop-down) lists to indicate the various levels of privacy.
- Make use of the 'just-in-time' notice. At the time that the application makes use of the personal data, it must be made clear to the user what will be done with their personal data. Personal data may not be used until this has been stated. Depending on the risk, the child must also be encouraged to consult a parent before the new use of data is activated. At all stages of the user process, consider whether such a just-in-time notice would be appropriate.
- Prevent influencing techniques ('nudging'). For example, do not use any visually misleading information by presenting the buttons to choose for more data processing more prominently than those for data minimisation.
- Be transparent about the implementation of patches and updates, and any implications thereof for privacy.

- Metadata which are not directly visible for the user (and are not comprehensible to the child) must be removed. (See Privacy Patterns[17] of Jaap Henk Hoepman)
- Privacy Label is a practical tool for providing insight into the collecting, processing and sharing of data[18].

Always bear in mind the child's age when providing this information.

- Opt for child-friendly wording. This could include things such as diagrams, cartoons, illustrations, video and audio content, game elements and interactive content which draw the attention of children, other than written communication. Test this approach with children and ask them for input.
- If some standard terms and conditions can only be formulated in legal wording, consider putting a child-friendly explanation next to it.
- Make several versions of this information, bearing in mind the child's age. Make use of the tips in principle 3 (appropriate information about privacy for every age category) and as described below.

When informing children, we advise taking account of their development stage in accordance with the classification proposed in the British Age Appropriate Design Code (see also the annex for a detailed explanation per age category):

- 0 - 5: pre-literate and early literacy (use simple language, repetition, explain on the basis of rhythm and song with animals and people, use rhymes and riddles)
- 6 - 9: core primary school years (use stories about friendship, the creation of skills, daily incidents about someone's values and critical thinking capacity)
- 10-12: transition years (use of role models, tell stories about the influence of family, friends and media on the child, encourage children in their need to experiment at this age and dare to make independent choices)
- 13-15: early teens (use of role models, tell stories about the influence of family, friends and media on the young, encourage children in their need to experiment at this age and dare to make independent choices)
- 16-17: approaching adulthood (use of role models, tell stories about the influence of family, friends and media on the young, encourage children in their need to experiment at this age and dare to make independent choices)

[17] https://privacypatterns.org/patterns/
[18] http://privacylabel.org/

The above classification is made on the basis of evolving capacities, skills and interests of the child. If there is a chance that children who are younger than the intended age category will make use of your service, take account of that age category in your design.

Give children the opportunity to exercise their rights in the area of data protection; give this a prominent place in the design.

- Make these tools easy to use and age-relevant (think of a chatbot, whereby chats are automatically erased after they have ended). Make use of the tips in principle 2 (about attractive, clear explanation to children), the tips above and from the annex.
- Align tools to rights that they support, such as:
    - a 'download all my data' tool to support the right of access and the right to data portability;
    - a 'delete all my data' or 'select data to be deleted' tool to support the right to be forgotten;
    - a 'stop the use of my data' tool to support the right to restriction of processing and the right to object to processing; and
    - an 'edit' tool to support the right to rectification.
- Make it clear how children can make a complaint about the processing of their personal data (including to the supervisory authority[19]) or can easily report unlawful/compromising use of their personal information. Make sure there are mechanisms in which the progress of a complaint/request to delete (unlawful/compromising) personal information can be followed and create the option that children can state that their complaint or request is urgent. Take all information they provide into account. Provide procedures to be able to take action quickly if information which has been provided indicates an acute risk to the protection of personal data.
- For toys, make use of a recognisable symbol (or button) which children can find easily when they want to exercise their rights. In the case of a connected toy device, put the symbol on the packing.
- Make codes of practice by which you will be bound and the guidelines set out in such codes easily accessible to children, in an understandable manner (see principle 10).

[19] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/jouw-privacy-voor-jongeren

Relevant laws and regulations

Children's rights perspective

Transparency is in the best interests of the child (Article 3 (1) UNCRC) (see principle 1), because by being able to and learning to understand what happens in digital services, you know what the impact on you and your environment can be. In that way, you can exercise some degree of control by making choices in the use of digital services and the exercising of your rights. Transparency is relevant for, among other things, the right to be heard (Article 12), the freedom of information and freedom of expression (Article 13), the right to freedom of thought (Article 14), and the right to access to the media and to protection from harmful content (Article 17 UNCRC).

Transparency is about being informed about the chances and opportunities of digital services so that they can contribute to the well-being of children. However, children must also be informed about the possible risks and restrictions of digital services. These restrictions can, e.g., be geared to protecting children from harmful content (Article 14 (4) UNCRC). When informing children, account must be taken of the evolving capacities of children (Article 5 UNCRC) and the fact that something that older children understand may not be something that younger children can get their heads around. Offering transparency with regard to the digital services must therefore also be geared to informing parents, guardians and others who support children.

Data protection legislation

The principle of transparency is one of the basic principles of the GDPR (Article 5 (1)(a) GDPR). The principle "concerns, in particular, information to the data subjects on the identity of the [provider] and the purposes of the processing and further information to ensure fair and transparent processing in respect of the [user] concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. [Users] should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing" (recital 39 GDPR). The transparency principle is elaborated in Sections 1 and 2 of Chapter III of the GDPR and encompasses provisions on the right to information (how and when what information on the data processing must be provided) (Articles 12-14 GDPR) and on the right to access of users (Article 15 GDPR).

As to the manner of providing information (the how), note the following points of attention: "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be

provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising" (recital 58 GDPR).

The following consideration is particularly relevant for this code: "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand" (recital 58 GDPR; Article 12 GDPR). It is important to read this together with the suggestions for the method of presentation of information, as some children might have a preference for text, but many children probably prefer more visual information (videos, games, comics, icons, etc.). Account must also be taken of the evolving capacities of children (Article 5 UNCRC) and the information will thus have to be suitable for children of various ages. Attention must be paid to word and language use and style to ensure that children genuinely feel addressed (see principle 2).

Consumer legislation

The principle of transparency is also relevant in consumer legislation. You can only make an informed decision about a transaction (e.g. an in-app purchase) if know exactly what the costs and functionalities are (see, e.g., Article 6:230m DCC). The best interests of the child (see principle 1) can mean presenting the information in a manner which is understandable and recognisable to children if it is likely that a transaction option will also be used by children. Bear in mind that children can only validly conclude contracts with their parent's consent (Article 1:234 DCC).

If you are not transparent about the specific features or terms of a transaction, this can constitute an unfair commercial practice (Article 6:193b DCC). A commercial practice is unfair if the user is misled, e.g. by giving factually incorrect information (Article 6:193c DCC) (see principle 8). It is also misleading not to mention information which is essential for making an informed decision on a transaction (Article 6:193d DCC). Specific account must be taken of what vulnerable consumers, in particular, might have understood, if a digital service was (in part) developed for them.

Principle 5: Carry out a privacy impact assessment based on children's rights

Explanation

If there is data processing which forms a potentially high risk, you must first carry out a privacy impact assessment (PIA). There can be a high risk, e.g., if users are profiled (see principle 7) or their conduct is systematically followed.

There is always a high risk when it comes to children, as the vulnerability of the person whose data you are processing is a criterion on the basis of which processing can be deemed risky. This is the case because the power relationship between provider and user is (even) more lop-sided if there are factors which make the user vulnerable. Vulnerable users, including children, may decide to consent or object to data processing without being fully aware and without proper consideration. It is therefore advisable to conduct a PIA as standard with digital services which will probably be used by children.

The goal of such a PIA is to chart what data is processed in what manner and what risks (for the rights and freedoms of the person whose data are concerned) this may entail. With children, it is logical that such an assessment will also take account of their specific fundamental rights. You will then have to determine with what measures you can effectively deal with the risks. When taking measures which have an impact on children, their rights and personal data, you will have to take account of their specific interests (see principle 1).

Implementation

Use the guidelines of the Dutch Data Protection Authority[20] and the European regulator[21] for the carrying out of a mandatory PIA.

In any event, a privacy impact assessment based on children's rights should contain the following seven steps (the following examples come from the British Age Appropriate Design Code[22]):

- Step 1. Identify when to do your PIA.
    - Complete the PIA before launching the service
    - Carrying out a new PIA is mandatory if you make important changes to the processing activities.
    - Also carry out a new PIA in the case of an external cause like a new security flaw, or new risks to children.
- Step 2. Describe the processing (nature, area of application, context, goal of the processing). Address the following questions in this respect:
    - whether you are designing your service for children, and if not, whether children are nevertheless likely to use your service;
    - the age categories of those children;
    - any plans you may have for parental supervision;
    - any plans you have for determining the age of your individual users;
    - the intended benefits for children;
    - the commercial interests (of yourself or of third parties) which you have taken into account;
    - any profiling or automatic decision making;
    - geolocation elements; the use of influencing techniques ('nudging');
    - processing special categories of data; processing of inferred data;
    - current issues of public concern relating to online risks to children;
    - relevant standards and codes of practice in the industry;

[20] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia
[21] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf
[22] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/?q=participation

    - relevant guidelines or research relating to the development needs, the well-being or the capacity of children in the relevant age category.
- Step 3. Consult with children and parents (see principle 2)
    - Consider whether you should seek independent advice from experts in the area of children's rights and development needs.
- Step 4. Assess necessity, proportionality and compliance relating to the collecting of personal data. Review the following points
    - the lawful basis for processing;
    - the condition for processing any special category data;
    - measures to ensure accuracy, avoid bias and explain the use of AI; and
    - specific details of the technological security measures (e.g. hashing and encryption standards).
- Step 5. Identify and assess risks to children. Study in particular whether the processing of personal data can cause, permit, contribute or in other cases can in fact help avoid the following risks:
    - physical harm;
    - stereotyping or discrimination of children or others;
    - online grooming or other sexual exploitation;
    - social anxiety, lack of self-esteem, bullying or peer pressure;
    - access to harmful or inappropriate consent;
    - misleading information or undue restriction on information; encouraging excessive risk-taking or unhealthy behaviour;
    - undermining parental authority or responsibility;
    - loss of autonomy or rights (including control of data, risk of provision of the child's personal data by someone other than the child, and privacy relating to third parties, including parents);
    - compulsive use or attention deficit disorders;
    - excessive screen time;
    - interrupted or inadequate sleep patterns;
    - economic exploitation or unfair commercial pressure; or
    - any other significant economic, social or developmental disadvantage.
- Step 6. Identify measures to mitigate those risks. Review whether you can reduce or avoid the risks you have determined in the design or whether you should add additional safeguards.
- Step 7. Record the conclusion. If your organisation has a data protection officer, you have to record the results and any measures of the PIA. It is recommended to publish the results.

A PIA is not a one-off exercise, you will have to continually assess the impact of the digital service on the rights and freedoms of users. The continued development and the use of a digital service can change the impact of the service and may require modification of the safeguards.

Relevant laws and regulations

Children's rights perspective

A privacy impact assessment based on children's rights is really a special form of the child impact assessment which the 'best interests of the child' principle requires of digital service providers (see principle 1). The PIA is intended to elaborate in a careful manner - i.e.: subject to effective safeguards - the right to data protection and privacy of children (Article 16 UNCRC, Article 8 ECHR, Articles 7 and 8 EU Charter). Such safeguards may not, however, constitute an unwarranted restriction of other rights of the child, such as their right to freedom of information and expression (Article 13 UNCRC) and to freedom of association (Article 15 UNCRC), or an infringement of other rights, including their right to protection from discrimination (Article 2 UNCRC). Thus if a digital service is likely to be used by children, a PIA which is based on children's rights should be carried out in conjunction with the child impact assessment discussed in principle 1.

Data protection legislation

As a provider of a digital service you must, in certain cases, carry out a privacy impact assessment or PIA (also called a data protection impact assessment) (Article 35 GDPR). This entails that an assessment must be made of the impact of data processing with a potentially high risk for (the limiting of) the fundamental rights and freedoms of the user of the service. This thus concerns other rights than the right to data protection, and for children more specifically their special rights. A PIA must be carried out if use is made of new technologies, the drawing up of profiles of users and the continual and systematic online following of their behaviour. Assume that if children are involved a PIA is mandatory.

Children are not mentioned, but processing data of persons who are deemed vulnerable, constitutes a high risk because of the possible extra lop-sided power relationship. Children fall in the category of vulnerable persons (recital 38 GDPR) and it is therefore advisable - and probably mandatory - to carry out a PIA if children can use the digital service. In any event, the interests of the child require an impact assessment and that principle and other children's rights must be taken into account when a digital service is likely to have an impact on children (see principle 1). The expectations of children and parents as interested parties must be included in the PIA (Articles 12 and 18 UNCRC) (see principle 2).

The PIA must also consider broader risks which the processing can pose to the rights and freedoms of children, such as the risk of significant material, physical, psychological or social harm. In addition, account must be taken of the different ages, capacities and development needs of children (Article 5 UNCRC). It can also be determined in a PIA what steps have to be taken to verify age and parental consent both adequately and in a privacy-friendly manner. A PIA can also answer the question whether the restricting of the freedom rights of children (such as the freedom of children to learn, to develop and to discover) with an eye to safeguarding their protection rights is proportional. Think of the situation in which children are only excluded from (a part of) a service if this is demonstrably or presumably harmful for them. In this respect, their evolving capacities and age must be taken into account (Article 5 UNCRC).

The use of a PIA has benefits for both the digital service provider and for children. For the processor, a PIA can in the end have a cost-saving effect, because from the start of the design process adequate account can be taken of data protection, as well as of other fundamental rights. This is possible through such things as adequately including data protection in the design of the digital service. Reputational damage can also be prevented at a later stage. A PIA can have a comforting effect for children and parents, because in the design stage attention is demonstrably paid to the interests and the rights of children.

Principle 6: Provide a child-friendly privacy design

Explanation

You may not process more personal data than is strictly necessary to achieve the specific goal of your digital service (for example providing a chat app). In other words, you are obliged to include privacy in the design of your app or game (privacy by design) and to align the default settings as privacy friendly as possible (privacy by default). In the best interests of the child (see principle 1), it is advisable to give this obligation shape in a child-friendly manner in the design. Child-friendly privacy design can also contribute to other privacy principles (think of safety and integrity) and the protection of the data protection rights of children.

Outside of minimising the number of personal data to what is truly necessary (but sufficient) for the specific purpose of your service, you can implement privacy in the design in other ways in a child-friendly manner. You can make data flows and choices in the use of personal data transparent in a child-friendly manner (see principle 4) and allow children to inspect their data processing in a simple and understandable manner in their data processing. The young people who provided input during the drawing up of this code, unanimously want to inspect what information about them is online ("**because it is important to know what information other people can see about you [...] so that I will know for next time what I should or should not accept**"), and indicated that they want to be able to control this.

In addition, you can build in options to easily delete data (the right to be forgotten). Young people we asked would make use of the option of deleting all their photos and details from an account (as long as there is some other way to store them), "**because then that information cannot just be used without my permission**". In addition, you can build in the option that you can object in an accessible manner to direct marketing (see principle 3) and you can withdraw your consent just as easily as you gave it (see principle 3). It is also advisable to design the digital service in such a way that children are *not* profiled by default (see principle 7). A child-friendly privacy design contributes to the realisation of other principles in this Code and the trust that children and parents have in the service.

Implementation

The results of the PIA (see principle 5) to remove the risks for the processing of personal data or reduce the risks as much as possible will, where possible, be included in the design of the service.

Make use of default settings for a child-friendly design.

- Choose an 'opt-in' regime as the default settings (privacy by default). Make sure that settings are as privacy-friendly as possible by default.
- Make sure that the default settings of your service are appropriate for children of all ages, i.e. the default settings have the highest 'protection level', unless it is possible to differentiate by different ages of children. For younger children, choose the highest 'protection level', while teenagers, for example, will have more freedom. In the latter case, it is good to know what their experiences with your service are and whether they require adjustment of the 'protection level'.
- Every form of optional use of personal data (including by third parties), including every use for the purpose of personalising the service, must be individually selected and activated by the child. An exception to this rule is if you possess a demonstrably compelling reason to opt for another default setting, e.g. when the best interests of the child are at issue.
- Consider building in measures for the time that a child tries to alter the default setting in a manner which might affect his or her safety, e.g. a warning when a user wants to make his/her profile 'public'. Carrying out a PIA for children (see principle 5) can help in this respect.
- Give the child the choice to permanently make use of these settings or to only decide on them per individual session. Make sure that the default settings are retained following software updates. Preferably do not use automatic updates, but let the child - or the parent/guardian - give explicit consent.
- Make it possible to set different user options on devices which are used by multiple users. Make sure that the protection of data is safeguarded on all devices where your service can be used.
- Upon purchase and installation of toys connected to the internet, provide clear information on the use of personal data. Equip the device with functions which make it clear for the child or the parent when you are collecting personal data.
- Make it possible when using a parent account to provide the parent with insight into the measures, including default settings, which have been set with the related child accounts.

- Do not collect any data if the application or the toy is not being used; at the end of the user session, the access to data and internet connection must be switched off.
- Include an easily accessible 'delete all my information' button (as explained under principle 4) that children can use at any time. Data must also be automatically deleted if the child removes the application.

Make sure that the geolocation, microphone and camera are turned off as the default setting and have children and/or parents give manual consent before they are turned on.

- After the end of each session in which the geolocation is used, the option must be turned off again.
- At the time that the child makes use of geolocation, this must be made clear to the child, at all times: i.e. at the time of subscribing, every time that that service is opened. Make sure that the child cannot unintentionally or by accident leave geolocation on.
- If you want to link the application to a location, consider requesting the location in some other way than via geolocation (e.g. by filling in the neighbourhood/city district).

Make use of techniques which benefit the privacy of children. Do not use nudge techniques to persuade or encourage children to activate options which are not in their interests or entail that you receive more personal data from them, or to turn off privacy protection.

- Give children the option of making use of the service under a pseudonym or to anonymously make use of your platform.
- Make use of VPN (or ORBOT or TOR) as default when starting up an app.
- Make sure that the child receives a clear, striking signal when he or she is being monitored or followed (even if a parent is watching).
- Use dummies. Dummies make use of the website and cannot be distinguished from real users. Children using a service involves a lot of privacy-sensitive information. This conduct can be 'hidden' by 'mixing' it with the use of fake users.
- Regularly delete cookies, e.g. when starting up the operating system, by switching them on per case, by determining whether the visited website is or is not trustworthy, and by only accepting a cookie for the current session. See also the website for Privacy Patterns of Jaap Henk Hoepman[23].
- For practical tools and guidance for the elaboration of Privacy by Design, see the PbD framework on the Privacy Company website[24].

[23] https://privacypatterns.org/patterns/
[24] https://www.privacycompany.eu/knowledge-base-nl/privacy-by-design-framework

Involve the relationship of children to their parents in a child-friendly design. Children have a right to privacy, including with regard to their parents. Where relevant this can also apply to other adults who deal with children, including tutors and teachers.

- Certainly when it comes to teenagers, it is advisable to give them an option to authorise having a parent watching, instead of building this in as default.
- Younger children can have a need for privacy. If an environment has been made safe for them or if parents can make advance choices based on their age regarding what children can see, they should be able to 'hang around there' and play without supervision. Within the application, consider designing an area that is not accessible to parents or other guardians. Make sure that the child part of the application is not open for communication with unknown persons, including persons with malicious intent.

Relevant laws and regulations

Children's rights perspective

According to the UN Committee on the Rights of the Child, the best interests of the child are particularly relevant because digital technologies were not (originally) designed specifically for children, whereas they are now used by many children in their daily lives. When designing digital services, account will therefore have to be taken of the best interests and the rights of the child, in particular the right to privacy (Article 16 UNCRC, Articles 7 and 8 EU Charter). In particular privacy and safety, including end-to-end encryption, must be part of the design of digital services.

Furthermore, the Council of Europe acknowledges that children's right to privacy and data protection not only apply in the relationship to digital service providers, but also in the relationship between children and their parents and guardians, peers and teachers. These rights could also be built in by design by, e.g., giving teenagers control of the privacy settings in educational apps used by parents. In the case of preventive or advisory services, it is relevant to safeguard the privacy of children with regard to others, including their parents. Children must have the option of discussing sensitive subjects in good faith with, e.g., a counsellor, certainly because the home situation is not always safe. The design of an app can also have unwanted side effects, such as abuse of unintended shared location details of children, which must in any event be prevented (see principle 5).

Data protection legislation

The basic principle of minimal data processing, also known as data minimisation, entails that the processing of personal data must be limited to a minimum. The data processing must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5 (1) (c) GDPR). This means, among other things, that the storage period of the personal data must be kept to an absolute minimum (recital 39 GDPR). The principle does not stand alone and is connected to other basic principles, such as the principle of legitimacy, the purpose limitation principle, the principle of storage limitation and the duty of accountability (Article 5 GDPR).

The principle of minimisation of data processing can be implemented by taking account of the principle of data processing by design (also called data protection/privacy by design) and of data protection by default settings (data protection/privacy by default) (Article 25 GDPR).

The obligation of implementing the principle of *privacy by design* entails, among other things, that in the design of a digital service account must be taken of the principles of Article 5 of the GDPR (and thus not only the principle of data minimisation). The best interests of the child, whereby the bests interests of children are a primary consideration, means that when designing the digital service, particular account must be taken of children. An effective way of taking account of children in the design stage is possible by aligning the design to the perceptions, experiences and expectations of children. This requires studying these perceptions, experiences and expectations of (and with) children in different age categories (see principle 2) because the evolving capacities of children might require other measures per age category.

As digital service provider, you must take appropriate *technical and organisational measures* when determining the means for processing and the processing itself (Article 25(1) GDPR). An appropriate measure can be, e.g., pseudonymisation (Article 4 (5) GDPR), which entails that the processing of personal data is carried out in such a way that the personal data can no longer be linked to a specific user without additional data or special techniques being used. In addition, appropriate measures must be taken to ensure that only personal data are processed which are necessary for each specific purpose of the processing (Article 25 (2) GDPR). Such measures could consist of, for example:

- "minimising the processing of personal data,
- pseudonymising personal data as soon as possible,
- transparency with regard to the functions and processing of personal data,
- enabling the data subject to monitor the data processing,
- enabling the [provider] to create and improve security features" (recital 78).

The provider of a digital service must show that it complies with the principle of privacy by design and by default (accountability, Article 5 (2) GDPR).

Although the *privacy by design* obligation in the GDPR is not specifically geared to children, it offers interesting opportunities for realising the explicit goal of the GDPR, i.e. providing extra protection for children and their personal data (recital 38).

What are *appropriate* measures for children may not be the same as for adults. When determining and designing measures to safeguard the principles and rights in the GDPR, account must in any event be taken of the best interests of the child (see principle 1). Here you should think of such things as visualising data processing in a child-friendly way and including options which are accessible and understandable for them and which allow them to control the data processing. This can include what is important to children themselves (see principle 2). The UN Committee on the Rights of the Child calls innovation based on the best interests of the child an important step forward in the development of digital services. A privacy impact assessment geared to children can provide support in this respect (see principle 5).

A number of the topics set out below can serve as an example of options for precisely (but not exclusively) taking account of the privacy principles and rights with regard to children in the design. This is not an exhaustive list.

Age verification - As a provider of digital services, you must know whether children are making use of your service for two reasons. First, you must know whether the users of your service are younger than 18 because, in that case, specific data protection (recital 38 GDPR) and an interpretation of the GDPR in the interests of the child (Article 3 (1) UNCRC) is required (see principle 1). Secondly, in the event that consent is used as a legal basis, it must be determined whether a child him- or herself can give consent (child is 16 or older) or whether parental consent (child is under 16) is required (see principle 3). In both cases, it is not permitted to process more personal data than is necessary to enable age verification.

Right to be forgotten - On the basis of the GDPR, there is a right to data erasure, also called the right to be forgotten, e.g. when data are no longer necessary for the processing purpose, the user of the service withdraws consent or lodges an objection (Article 17 GDPR). The right is particularly in the best interests of children, because they may have shared data when they were not yet (sufficiently) aware of the processing risks and they wish to remove these data (from the internet) later - including when, or precisely because, they are no longer a child (recital 65 GDPR). You do not want children to be plagued by the transgressions of their youth. At a certain point in time it must be possible for them to start with a clean slate again. If someone requests erasing of data that was provided when he or she was a child, then as digital service provider you must comply with these wishes as much as possible. This particularly applies if it is likely that they provided their personal data without fully understanding the implications. In addition, you must inform the third parties to whom the personal data have been provided as to the request for erasure. If children may give consent themselves or exercise their rights themselves, a request of a parent (or other legal guardian of the child) to delete data may not be

fulfilled without involving the child. As it must be possible to easily erase data if users are entitled to this, it is advisable to include this in the design of the digital service. Take account in this respect of the fact that it must be possible to withdraw consent as easily as it is to give consent, and the withdrawal of consent is a ground to immediately erase data.

Right of access - the user of a digital service has the right to access personal data which is being processed with regard to him or her (Article 15 GDPR). This is a right that must be able to be exercised "easily and at regular intervals" (recital 63 GDPR). By allowing access to data processing by means of, e.g., a privacy dashboard, the design of the digital service immediately takes account of the right. This gives shape to the right to information and to access at the same time.

Security - it may speak for itself, but the obligation to adequately secure personal data (Article 32 GDPR) is something to be borne in mind when designing a digital service. Be sure to engage children themselves (see principle 2) to determine whether they encounter specific vulnerable situations and have specific wishes. An interesting phenomenon is sharing login data with friends: something that is at odds with safe internet use, but does meet a social need. It is thus good to pay attention to this and to investigate whether the two can be reconciled with each other in some way, so that what is deemed to be socially desirable, does not undermine the safety of an app or game.

Principle 7: Prevent the profiling of children

Explanation

“I believe an app is harmful if it harms minorities”
- a young person who participated in a session for drawing up the Code.

Profiling of users is seen as high risk processing which requires, e.g., a PIA (see principle 5). In addition, there are restrictions when profiling children. They enjoy extra protection when drawing up user profiles and personality profiles. Profiling happens for a range of purposes. For example, you can use it to offer individualised marketing and services or to distinguish interesting customers from customers who form a risk for a business.

Profiles can be made on the basis of data collected about persons or groups of persons. Often this concerns online or offline data on behaviour. Preferences or characteristics of persons can be inferred from that data on the basis of associations with other users. The picture that this creates of a user can be very invasive and privacy-sensitive. What is more, the picture does not necessarily correspond with reality if it is based on correlations. This encompasses the risk that someone might be labelled incorrectly. This can be harmful as it leads to stereotyping, stigma and unwanted or unfair treatment (e.g. biases or incorrect exclusion from services) or even discrimination of persons.

Children are seen as vulnerable when it comes to profiling. Profiles of users become more accurate when they spend a lot of time on a digital service or keep returning to it, so that as many behaviour details as possible can be collected. This can lead to obsessive use, so that children, e.g., spend less time on school work or are continuously disrupted while learning and their school results come under pressure. In addition, children may be more easy to influence. Vulnerabilities can be used for marketing purposes in a manner that is at odds with their freedom of information, freedom of thought, or their right to a place to play and engage in recreational activities free of commercial messages. Lastly, the long-term effects of profiling of children are often not sufficiently known.

Implementation

Make sure that profiling functions are turned off by default, unless there is a compelling reason for profiling in the best interests of the child.

- A compelling reason is, e.g., that profiling is necessary because for the benefit of children's well-being you must comply with specific laws and regulations (for example, to prevent sexual exploitation and abuse).

If you are nevertheless forced to profile, take the following measures:

- Make it clear why profiling is in the best interests of the child (see principle 1).
- Make clear what type of profiling is used for which purpose. Where appropriate, there must be separate privacy settings for every form of profiling. Different forms of profiling may not be placed under one and the same privacy setting.
- There must be appropriate interventions at the point where profiling is to be switched on (for example, age-relevant information on what happens with the personal data of the child, possibly encouraging the child to have an adult joint him or her depending on the child's age)
- Take appropriate measures to safeguard that this will not result in any psychological or physical harm to the child. Test the effects of the method of profiling on the basis of (human) moderation and reporting procedures.
- Assess whether profiling has any effects which harm the best interests and rights of the child. Provide specific safeguards to protect the best interests and rights of the child (see principles 1 and 5).

Relevant laws and regulations

Children's rights perspective

Both the Council of Europe and the UN Committee on the Rights of the Child call for great reserve by prohibiting the online profiling of children, unless this is in the interests of the child. The choice for such an approach is understandable because the (long-term) impact of online profiling on children, including for marketing purposes, is still not known. Nor should there be profiling of children, unless this is in their best interests because it contributes to their well-being and the means used are proportional and do not unnecessarily infringe the (privacy) rights of children. There must be special attention for the child's right not to be subject to discrimination (Article 2 UNCRC). Decision making on the basis of profiling can lead to bias, stereotyping and discrimination of (groups of) people, including children. Discrimination can lead to tangible and intangible harm and is prohibited. In any event, the discrimination of parents as a result of profiling can have an impact on their children.

Data protection legislation

Profiling encompasses every from of automated processing of personal data to assess personal aspects of a user, in particular analysing or predicting characteristics such as performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of the data subject (recital 71 GDPR). Profiling can be used for a range of purposes, such as providing person-oriented content or marketing or the personalising of digital services.

Children merit extra protection because they are less able to estimate the risks of data processing. This is particularly recognised with regard to the creation of personality or user profiles (recital 38 GDPR). The GDPR therefore considers that profiling may not relate to a child if it has legal consequences or relates to children to a significant degree (recital 71 GDPR). On the basis of the basic principles of lawfulness, fairness and transparency (Article 5 GDPR), a digital service provider must be cautious in its profiling. Profiling is generally not immediately visible to the user so that it is difficult to understand what is actually happening and what the consequences will be. For children this is even more objectionable. Not only because sufficient understanding of the situation is lacking, but also because they are less able to oversee the (long-term) consequences.

Profiling is not permitted if legal consequences are attached to this for someone or it affects him or her to a significant degree in some other way (Article 22 GDPR). A user has the right not to be subject to an automated decision, including profiling, without human intervention. Without human intervention means that a decision comes directly from the computer itself and there is no longer any meaningful monitoring by a human to review whether the decision is correct.

The chance that profiling relates to someone to a considerable degree can be greater for children due to their vulnerability. There will be an ‘affect to a significant degree’ if profiling is harmful for the development of children. This can be the case with personalised marketing. Profiling of children for marketing purposes is therefore not recommended. In any event, no actual effect need be shown to be able to speak of a significant impact.

There are also exceptions to the profiling prohibition in Article 22 GDPR. An exception can be, e.g., that the user of a service has explicitly agreed to profiling or if it is necessary for the performance of a contract (Article 22 (2) GDPR). It is assumed that these exception grounds relating to children must be interpreted restrictively and profiling may only be permitted if this is in the best interests of the child. There can be such an interest if profiling contributes to the health or the education of the child. In that case too, appropriate safeguards must be established for children to protect their rights.

Principle 8: Avoid the economic exploitation of children at all times

Explanation

Children have the right to play and engage in recreational activities in an environment which is free of commerce. However, digital technology (which is used for games and recreational activities) is provided by businesses for commercial purposes. Obviously businesses are entitled to earn money with their app or game but, if they are used by children, there are some special points for attention to prevent economic exploitation.

Digital services often generate income with in-app purchases. With children it is important that in principle they may only make a contract with their parents' consent. Children are also sometimes intentionally tempted or misled to make choices, e.g. purchasing extra lives or levels if they get stuck in a game, which looking back they would rather not have made. The actual value of in-app purchases can also be obfuscated, because games use their own virtual currency.

In addition, in-app purchases can have an element of gambling so that the dividing line between gaming and gambling becomes ever less clear. Think of things like virtual packages with secret contents (loot boxes or blind boxes) which are purchased with real money via micro-transactions. The temptation of loot boxes can be great if there is a chance that the contents (e.g. a powerful weapon) can help to improve performance in a game or where a special costume makes the game character of the user more popular.

All these kinds of practices are particularly intended to serve the commercial interests of the digital service. We therefore also call it exploitation-oriented design of digital services or 'dark patterns'. Not only is the commercial interest paramount, it also undermines the autonomy of the users of a service in making their own choices. The information asymmetry between provider and user of a digital service is increased because customers are often not aware of the working and the goal of dark patterns which are let loose on them. They do not always see what the impact on their actions is and what the possible risks are. Dark patterns can consequently be misleading, unfair and unlawful.

In addition, exploitation-oriented design of apps and games can be part of personalised, data-driven marketing. This is a form of marketing which functions as an earnings model for many apps or games and benefits from processing a lot of data. Due to the design of an app or game, the user is, for example, "seduced" into spending a lot of time there so that a large quantity of behaviour data about him or her can be collected. Settings for a privacy-friendly use of apps

and games can also be hidden or made needlessly complicated so that they are difficult to use for the user, and certainly for children.

All these collected behaviour data can create a very invasive picture of someone. In addition, characteristics about (groups) of people can be inferred (profiling) (see principle 7). These profiles say something, for example, about a person's personality, sexual identity, emotional state, medical condition, interests, needs and social contacts. People themselves become the means for generating profit, as these data and profiles represent an economic value. This is particularly problematic for children, as they must be protected from economic exploitation.

Another example of the economic exploitation of children is the algorithm-driven information provision on, for example, video platforms. The user must spend as much time as possible behind the screen to maximise ad income. A tried-and-tested method for amusing users (and thus keeping hold of their attention for as long as possible), is recommending ever more sensational content. With the autoplay function, the user no longer has to think about the next video they want to see. The algorithm determines this on the basis of your viewing history and automatically starts playing the next one. According to the young people who provided input, when drawing up the Code, 'autoplay' should be one of the first functions abolished by a video platform.

Implementation

Do not make use of advertising which in word, sound or picture can mislead children in some way. In addition, advertising may not, cause formal or physical harm and must therefore:

- not encourage the purchase of a specific product by benefiting from the inexperience or gullibility of a child;
- not directly encourage the child to convince parents or others to purchase products which are advertised;
- not profit from the special trust that children have in parents, teachers or others.

Furthermore, advertising directed at children may not suggest that having or using a specific product will give them a physical or social advantage compared to other children, nor that not having a specific product will lead to the opposite effect. Concretely for the design of a digital service, this means that, e.g.:

- In case a website makes advertising geared to children visible via a banner and/or via a pop-up, the ad must be accompanied by the statement of the word "ad" or "commercial" which is immediately clear at one glance.
- Advertising in posts and other ads must be clearly recognisable by optical, virtual and/or acoustic means, appropriate for the comprehension powers of children.

- It is not permitted to directly encourage children to advertise on behalf of the advertiser.

Designers should be aware of the Dutch code for advertising directed at children and young people (Kinder- en Jeugdreclamecode[25]) and the Social Media and Influencer Marketing Code[26].

Be transparent about purchases or other commercial aspects of a game:

- Only call a game 'free' when it is completely free of charge. For example, games with in-app purchases may not be sold as 'free'. Before the purchase, make it clear to the potential user whether in-app purchases are possible. When creating the design, the preference is for a one-off payment in advance (instead of continually in-app).
- If there are nevertheless in-app purchases, this must be explained in clear language (e.g. with universal symbols for purchases). Mention the currency in euros with every invitation to purchase, instead of only in the unique currency of the app or game. And repeat 'this costs real money' or a comparable message at the time that it applies, e.g. at the time of the purchase itself.
- If a game or app is primarily played by children, consider whether payment settings can be given form in such way that children cannot make any purchases without parental supervision. You can do this, for example, by requiring a password for each purchase or for purchases above a specific amount.
- Let the user of an 'early access' game know immediately at the start what he or she is starting. It should be clear for the user that the game will not feature further development. It should also be clear to the potential user when the game has been an 'early-access' game for a longer period of time or is (possibly) no longer being developed.

See the guidelines in the Protection of Online Consumers of the Netherlands Authority for Consumers and Markets[27].

Avoid the use of loot boxes or other techniques which are used to encourage purchases by users, such as offers which are only valid for a limited time, hidden advertising, micro-transactions, use of other currencies, price personalisation and algorithms which determine the best sales strategy.

[25] https://www.reclamecode.nl/nrc/kinder-en-jeugdreclamecode-kjc/
[26] https://www.reclamecode.nl/nrc/reclamecode-social-media-rsm/
[27] https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument

Let the content that children create on, e.g., video platforms and in social media apps, remain the property of children themselves. Relevant laws and regulations

Children's rights perspective

Children are entitled to protection from economic exploitation (Article 32 UNCRC). Economic exploitation is taking unjust advantage of children for a businesses own benefit. This can also include the manipulation of children to achieve economic benefit, including by the exploitation-oriented design of digital services. The UN Committee on the Rights of the Child views this as a lack of respect for the harmonious development of a child's personality. Exploitation-oriented design is not in the best interests of the child (Article 3 UNCRC) if it does not contribute to their well-being or is in fact harmful to them. It concomitantly has an impact on the right of children to optimal development (Article 6 UNCRC). In addition, when it comes to economic exploitation, the best interests of the child are not a primary consideration, but rather the interests of the business itself.

Exploitation-oriented design also touches upon a child's right to privacy and data protection (Article 16 UNCRC), Articles 7 and 8 EU Charter) if it is accompanied by unnecessary or even excessive data collection. The manipulation of their thoughts with content selected on the basis of algorithms can be contrary to their right to freedom of information (Article 13 UNCRC) and freedom of thought (Article 14 UNCRC). Exploitation-oriented design has an impact on their right to rest and leisure (Article 31 UNCRC).

The Council of Europe argues for measures[28] to protect children from economic exploitation in the use of digital services. Advertising and marketing must take account of the age of children. Children who are not yet ready for this because of their age deserve protection. With regard to children who are at an age when they recognise advertising and critically reflect on it, it is, on the other hand, important that they learn to deal with it and this may fall under their right to freedom of information (Article 13 UNCRC). It is important that it is very clear when something is intended as advertising or marketing. The UN Committee on the Rights of the Child calls for significant reserve when it comes to new forms of marketing because they may be contrary to the rights of the child.

Advertising and marketing strategies are becoming more and more sophisticated in influencing users, e.g. by bombarding them continually and on various platforms with advertising, or by using hidden tactics and/or tactics geared to emotions, such as advergames, brand pushers

[28] https://rm.coe.int/09000016808d881a

(including children) and branded pop songs, so that advertising and marketing become inescapable. Older children's cognitive defences to this are just as poor as those of younger children. If transparency with these forms of marketing does not help to protect children against negative effects (think of unfair manipulation), the 'best interests of the child" principle (see principle 1) and the child's right to development (Article 6 UNCRC) are not being met. The UN Committee on the Rights of the Child mentions as examples of marketing which can be contrary to the rights of the child: data-driven, targeted marketing on the basis of the personal and location information of children which are generated across platforms. This applies all the more if this is accompanied by marketing-oriented design choices which send children to more or more extreme content or with automated, sleep-disrupting notifications. According to the UN Committee on the Rights of the Child, some forms of marketing should be prohibited, including the targeting of children, regardless of their age, on the basis of profiles as well as neuromarketing geared to children.

Data protection legislation

In the data protection legislation, children are entitled to specific protection, in particular in the use of their personal data for marketing purposes or for the drawing up of personality or user profiles (recital 38 GDPR). They are less capable of recognising marketing practices and assessing them critically, certainly when they are accompanied by (usually) not immediately visible data processing and profiling. It must be prevented that abuse is made of the lack of awareness on the part of children of the operation and the possible consequences of these forms of marketing. The GDPR does not contain a general prohibition of marketing geared to children, but there are clear limitations of data processing for marketing purposes.

Consent and marketing - if data processing for marketing purposes becomes an obligatory part of an app or game, but does not belong to the core of the service, consent for the use of that digital service will not have been given freely. You have no free choice whether or not to agree. In such a case, consent will not have been validly given (Article 7 (4) GDPR) (see principle 3). In addition, consent must be informed and in the case of children that information must have been presented in an manner that they can understand and recognise. However, data-driven, targeted marketing practices are difficult to explain to children, so that it is doubtful whether they can give consent for this in an informed manner if they are themselves authorised to give consent (Articles 7 and 8 GDPR). In any event, you can also wonder whether these practices for adults - and consequently the parents of children - are always sufficiently understandable. It can help to keep the data processing as simple as possible.

Legitimate interest and marketing - data processing for direct marketing purposes can be a legitimate interest of the digital service provider (recital 47 GDPR) (see principle 3). However, this data processing must have a minimal impact on the user's right to privacy. Moreover, in the case of children, the best interests of the child must be a primary consideration when weighing

the various interests (see principle 1). If, on the other hand, there is substantial data processing, such as when creating profiles, the sharing of data with data brokers, behaviour-based marketing and online direct marketing, then consent (Article 6 (1) (a) GDPR) might be a more appropriate legal basis. The basic principles of the GDPR must always be satisfied, including the principle of minimal data processing (Article 5 (1) (c) GDPR).

Right to object and direct marketing - as a user you can object to data processing for direct marketing (Article 21 (2) GDPR). The user must be informed about this, whereby it must specifically be borne in mind that information for children is understandable and recognisable.

Profiling and marketing - children particularly merit protection when drawing up personality and user profiles (recital 38 GDPR). Profiling as part of automated decision making is prohibited unless there is an exception ground (Article 22 GDPR) (see principle 7). Targeted or personalised marketing are forms of profiling which can be harmful for the development of children and the profiling of children for marketing purposes is not advised because it is likely that this will have a significant effect on them. This interpretation is also in line with the best interests of the child (see principle 1).

Consumer legislation

The exploitation-geared design of digital services can be an unfair commercial practice (6:193a DCC et seq.). A commercial practice is unfair if the user consequently makes a decision on a transaction which they would otherwise not have made. It must protect the user against practices which hinder them in making a well-considered and informed decision about an economic transaction. The (un)fairness of a commercial practice will be assessed on the basis of what the average consumer (in this Code the user of a digital service) can understand.

In the case of children, you should look at what the average member of the group of children could understand if the (in this case) provider focuses on this group or could reasonably foresee that this group could be affected by the commercial practice or the underlying product. The group can be specified, e.g. by age. A child can be the victim of a practice which the average adult consumer will mistrust. Factors are conceivable which might entail that an average child of a group may be less reasonably informed, cautious and alert. Social, cultural and linguistic factors play a role in this respect, but age also plays a role. If a provider focuses on children, then the provider must take account of the fact that children assess information in a different manner than adults. This means that children in vulnerable situations should have extra protection.

There are also commercial practices which are unfair and thus prohibited under all circumstances (Articles 6:193g and 193i DCC). There is a black list of misleading commercial practices and a black list of aggressive commercial practices. With misleading commercial practices, the provider in essence gives factually incorrect or misleading information, leaves

out information, or the provider is ambiguous about it. Examples of misleading commercial practices are offering a service as free while in fact there are costs connected with it, or incorrectly claiming that a product will only be available for a very limited time.

With an aggressive commercial practice the user's freedom of choice is significantly limited or can be limited in an inappropriate manner, by intimidation, coercion, including the use of physical violence, or inappropriate influencing. Examples of aggressive practices on the black list are having to pay to receive a prize that has been won (other than the necessary shipping costs to the child) or directly encouraging children through advertising to purchase a product, including virtual items in, e.g., games, or to persuade their parents to purchase the product for them. When assessing the unfair commercial practices, the entire context of a digital service must be taken into account, including the situational vulnerability of children.

Other laws and regulations

Advertising - A provider of a video platform must see to it that advertising, e.g., in the form of ads, sponsoring or product placements, are recognisable and do not use any subliminal techniques (Article 3a.5 (1)-(2) Dutch Media Act). Product placement is not permitted (Article 3a.5 (3) Dutch Media Act). A provider of a video platform on which there is advertising falls under the regulations and the supervision of Stichting Reclame Code (Article 3a.4 (1) Dutch Media Act). Apps and games also fall under Stichting Reclame Code. Stichting Reclame Code sets conditions for advertising to safeguard the credibility and reliability thereof. Advertising may not be misleading, needlessly hurtful or threatening, and must be legally permitted. For example, it is prohibited to affect human dignity, to discriminate and to encourage behaviour that is harmful to health, safety or the environment (see the Dutch Media Act and the Dutch Tobacco Act). There are specific Advertising Codes including for gambling[29], youths[30] and social media & influencer marketing[31].

Gambling - Gambling legislation seeks to protect vulnerable groups, including children[32]. In 2021 it will be possible for providers to apply for a permit for online gambling. Online gambling may not be offered to children (Article 31k (2) (a) Dutch Remote Gambling Act). Moreover, a

[29]https://www.reclamecode.nl/nrc/reclamecode-voor-kansspelen-die-worden-aangeboden-door-vergunninghouders-ingevolge-de-wet-op-de-kansspelen-rvk-2015/
[30] https://www.reclamecode.nl/nrc/kinder-en-jeugdreclamecode-kjc/
[31] https://www.reclamecode.nl/socialuitleg/
[32] https://kansspelautoriteit.nl/onderwerpen/minderjarigen/

permit holder (i.e. a holder of a permit to organise remote gambling) may not direct any registration and advertising activities specifically to children.

A clear distinction must be made between games and gambling. When providing remote gambling services, a permit holder may not provide any games or advertise them to children. In addition, the provider may not advertise in services where games are provided (see explanatory memorandum[33] with the Dutch Remote Gambling Decree[34]). In addition, the Dutch gaming authority, Kansspelautoriteit, has prohibited loot boxes[35] with which prizes which have an economic value can be won in games. The Kansspelautoriteit is also critical about other gambling elements in games. The consideration takes account of the fact that children are extra vulnerable because of their evolving capacities (Article 5 UNCRC) and could possibly be easily made more sensitive to gambling. Seen from the perspective of the best interests of the child, it is therefore advised to protect children against gambling elements in apps and games (see principle 1).

[33]https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/03/03/tk-bijlage-besluit-kansspelen-op-afstand/tk-bijlage-besluit-kansspelen-op-afstand.pdf
[34]https://kansspelautoriteit.nl/over-ons/publicaties/regels-leidraden/online-kansspelen/besluit-kansspelen/
[35] https://kansspelautoriteit.nl/onderwerpen/loot-boxes/

Principle 9: Avoid a harmful design for children at all times

Explanation

"**I think an app is harmful if it makes you neglect other things or if it makes you feel bad.**" - a young person who participated in a session for drawing up the Code.

In addition to design geared to economic exploitation, harmful design - in other ways - must be avoided at all times. Harmful design means, among other things, a design choice in a digital service which wrongly makes use of or abuses the vulnerability of children, or does not (adequately) deal with behaviour that can have a negative impact for children. Design is harmful if it has negative consequences for the health or the well-being of children. The well-being of children encompasses all aspects of their development, including their mental, social, cognitive and physical development.

Design can be harmful for the development of children if it inadequately protects them against possible harmful content, contacts or behaviour. In terms of harmful content, think of such things as the (automated) showing or glorifying of violence, stereotyping, racism, disinformation or pornographic content in an app or game. Harmful contacts or behaviour can relate to bullying, (sexual) abuse, incitement, hate speech, recruitment for criminal practices and radicalisation.

Furthermore, there can be design that has a possible negative impact on their social relationships. Think of such things as fixed times in games when children can make special achievements (like skins and weapons) so that other planned activities with, e.g., family or friends are disrupted. Another example is (temporary) exclusion from participation in a game when the game has to be interrupted to eat.

These kinds of mechanisms can lead to conflicts with parents and social peer pressure. If they are continually disturbed by notifications, it can also have a negative effect on the capacities of children to concentrate on other activities like their school work. Think of games which continually pull the player back in to ensure progress in the game. Design can also lead to excessive use of digital services and can even lead to health problems (including sleep deprivation, physical harm and compulsive behaviour).

Design choices whereby children are (subconsciously) forced into to a certain behaviour that they might not have shown without those choices, and/or which have a disruptive effect on their health, social relationships and other activities in their daily life, should preferably be

avoided. This is certainly the case if those choices can be shown to not be in their best interest or are harmful.

If it is assumed for specific forms of design that they do not contribute to the well-being of children or are harmful to them, but there is no (convincing) proof, then be cautious and do not use it in a service which will probably also be used by children. We call that the precautionary principle. This approach is based on the 'better safe than sorry' principle: if it is likely that the design could in some way have negative effects on children, it is better to be cautious with the implementation thereof.

Implementation

If it is likely that a specific design is potentially harmfully for children, you should apply the precautionary approach. Use the outcomes of the child impact assessment from principle 1.

Apply the following rules for the use of rewards, notifications and likes:

- Avoid using personal data in such way that children are encouraged to stay on longer, such as, in exchange for continuing to play for longer or offering children personalised in-game benefits (based on your use of the personal data of the individual user).
- Present options to continue playing or in some other way make use of your service in a neutral manner, without suggesting that children will be missing out if they don't. Try to reduce the time pressure by including fewer or no time-limited assignments (this can have an addictive effect).
- Avoid functions which use personal data to automatically extend the use, instead of letting children make an active choice as to whether they want to spend their time in this manner (data-steered autoplay functions).
- Introduce mechanisms like pause buttons, through which children can take a break at any time without losing their progress in a game, or provide age-relevant content to support making conscious choices about taking breaks.
- Limit the excessive use of notifications or make sure that they can be easily switched off.
- Make sure that children can stop using the application at any time (and can delete all their data, see also principles 4 and 5) without their having to feel guilty about this.
- Prevent incentives for children to add as many as possible (unknown) friends or followers.

Design the digital service in such way that users come into contact with harmful content, contacts or behaviour as little as possible.

- Promote and communicate the community guidelines of the design in a way which is appealing and appropriate for users of all ages. For example, community guidelines and codes of conduct which make it clear what behaviour is not welcome in your game or service.
- Provide mechanisms through which children can confidentially report inappropriate behaviour and infringements of the community guidelines, and make sure that they are easy to find and use.
- Be transparent about what content might be harmful for a specific age category and make sure that children can report this content if it might be harmful or illegal.

If the app or game encourages children to move in the physical environment when using an app or game, make sure this occurs in the safest possible manner.

- Make sure that children can move safely through their physical environment by, e.g., continually reminding them or making it clear as they play.
- If users are encouraged through the application to visit specific physical locations, make sure that these locations are appropriate for the development of the child (see also the classification per development stage under principle 2).
- If children are encouraged to meet other users offline, set this up in such a way that it is appropriate for the age of the child. For example, do not make profiles of children under a certain age openly visible to other users.

Relevant laws and regulations

Children's rights perspective

Protecting children from harmful design is directly connected with the best interests of the child: it is not in the best interests of the child that digital services make use of a design that is harmful for children or a design that does not sufficiently prevent harm to children. Children have a right to, among other things, an optimal and healthy development (Article 6 UNCRC), a right to health (Article 24 UNCRC), and protection from harmful content (Article 17(4) UNCRC). In addition, they have the right to protection from violence (Article 19 UNCRC) (including bullying) and from sexual abuse (Article 34 UNCRC).

Moreover, safeguarding the interests of the child entails that activities, including digital services, which have an impact on them, must contribute to their well-being. Harm must therefore certainly be prevented and if there is a likelihood of harm, a precautionary approach must be chosen, e.g., by not making a specific design choice. Account can be taken in this respect of the evolving capacities of children (Article 5 UNCRC): what is harmful for young children, need not necessarily be harmful for older children. In addition, certainly for older

children, it can be very educational to learn how to deal with the risks of digital services. For example, by letting them experience how design can influence them and teaching them how to critically review designs. Critical review does presume that children know that certain design choices can influence them and preferably also that they have the option of making a different choice. Learning to critically review design choices is not an obligation as such for designers and could become part of wider awareness activities relating to digital technology.

If safety measures are built into the digital service (safety by design) to protect children against harmful content or contacts, account must be taken of the evolving capacities of children (Article 5 UNCRC) and other children's rights, such as their right to privacy (Article 16 UNCRCR) and right to freedom of information (Article 13 UNCRC). Age verification (such as for gambling) or content classification (comparable to the parental guidance system[36] for audio-visual media or PEGI[37] for games) can be adequate instruments for protecting children, whereby account must be taken of the evolving capacities of children (Article 5 UNCRC).

Data protection legislation

Data processing to influence the behaviour of users or show specific content must demonstrably satisfy the data protection legislation. (see principles 3, 4, 5, 6). From the perspective of fairness (Article 5 (1) (a) GDPR), there must be specific attention for data processing whereby the personality, including the vulnerability, of the child is used in the design and use of the digital service. For example, profiling of children is not permitted, unless it is in their best interests, e.g. because it contributes to their well-being (see principle 7).

When implementing safety by design instruments, it is required to demonstrate compliance with the data protection legislation (see principles 3, 4, 6, 7). If use is made of age verification to ensure that harmful content is not accessible to children of specific ages, account must be taken of the principle of minimal data processing (Article 5 (1) (c) GDPR) (see principle 5).

Other legislation

Removal of illegal information - providers of digital services have a duty of care to immediately remove unlawful information or make it inaccessible if they know or should reasonably know about the unlawful character thereof (Article 6:196c(4) DCC). There does not need to be a prior check in the storing and publishing of information on, e.g., a social media platform, but the provider does have a duty to investigate if there is a reason to doubt the lawfulness of stored information. The child porn reporting agency, Meldpunt Kinderporno, which is part of the

[36] https://www.kijkwijzer.nl/
[37] https://www.kijkwijzer.nl/pegi

Expertisebureau Online Kindermisbruik, the agency monitoring online child abuse, can help, for example, in the removal of child pornography.

Dutch Media Act and video platforms - providers of video platforms must take measures to protect children from content which is harmful to their physical, mental or moral development (Article 4.1a Dutch Media Act) and to protect users in general - children and adults - from content which incites violence or hate with regard to a person or a group of persons on the basis of religion, creed, political persuasion, race and gender, sexual orientation and disability, and against content, the distribution of which, constitutes a crime (e.g. racist content, child pornography, or content which elicits the commission of an act of terrorism) (Article 2.88 Dutch Media Act). The measures to protect users, and in particular children, against these three categories must be laid down in a code of practice (Article 3a.3 Dutch Media Act 2008). The platform must also ensure that users are informed of content placed by others, 'user generated content', which might be harmful for children. Video platforms will fall under the parental guidance system (Kijkwijzer)[38] of the NICAM.

[38] https://www.kijkwijzer.nl/

Principle 10: Develop industry guidelines which are geared to protecting the interests and rights of children

Explanation

More and more children are spending more and more time on digital technologies. These technologies are primarily developed and provided by the private sector. Consequently companies have an enormous impact on children and their rights. There is always the mandatory obligation to act in the best interests of the child (see principle 1). However, this requires awareness and can also be a challenging task, as the principles in this Code make clear.

The UN Committee on the Rights of the Child recognises that businesses can themselves contribute by drawing up guidelines or codes of practice. This can be on a voluntary basis. In addition, the law can encourage or prescribe these kinds of self-regulation by, e.g., industry organisations.

A code of practice makes it clearer for an industry as to how certain rules are to be explained to children so that their rights are properly safeguarded. Certainly for businesses which provide products and services for which it is likely that they will be used by children, like apps, games and connected toys, it is advisable to draw up guidelines with the industry. A code of practice is not without commitment and, as a business, you will have to adhere to it, as otherwise you could be deemed guilty of misleading commercial practice.

Implementation

- Consult guidelines from the relevant industry, examples of appropriate guidelines are the UNICEF Children's Rights and Business Principles[39] and the UNICEF Child Online Protection Guidelines for the ICT Sector[40].
- Engage children in drawing up guidelines and make sure that these are public, so that parents, teachers and children can read and understand the guidelines. Promote and communicate the guidelines in a way which is appealing for users of all ages.
- Make sure that there is actual compliance with the guidelines.
    - Make sure that the guidelines are carefully embedded in the relevant chain.
    - Make sure that compliance is regularly monitored.
    - Establish an (effective) enforcement mechanism.
- Making the interests of the child paramount is an iterative process: regularly assess whether new updates or developments are still in line with a child-friendly design. Preferably establish a process-based and recurring assessment which specifically focuses on the best interests of the child.
- Stay abreast of recommendations or advice in the relevant industry and where necessary tighten the guidelines.

Relevant laws and regulations

Children's rights perspective

A code of practice of an industry involved in digital services can contribute to the implementation of the 'best interests of the child' principle (Article 3, UNCRC) by drawing up effective codes of practice based on the rights of the child. By doing so it accounts for the choices which have been made in the application of the applicable legal rules when digital services have an impact on children. More specifically, the data protection legislation fleshes out the right of the child to privacy and data protection (Article 16 UNCRC).

The UN Committee on the Rights of the Child also points to the importance of codes of practice that "adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and

[39] https://www.unicef.org/csr/resources.html

[40] https://www.unicef.org/csr/files/Training_Module_2_Child_Online_Protection_for_ICT_industry.pdf

services" (General Comment No. 25). It must be monitored that businesses apply high standards for transparency and verification and any innovations regarding their measures are in the interests of the child. The UN Committee on the Rights of the Child points, in particular, to the importance of codes of practice for marketing.

Data protection legislation

Industries can make it clear by means of the drawing up of codes of practice how they flesh out the standards of the GDPR. A code of practice is a form of self-regulation by an industry organisation or association. In the case of the specific protection which children must have under the GDPR, a code of practice can be an important instrument in contributing to the duty to account (Article 5(2) GDPR) by describing in detail what behaviour rules apply in an industry.

Under the GDPR, the drawing up of codes of practices is encouraged, in particular with regard to children "so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors" and "In particular, such codes of conduct could calibrate the obligations of [providers], taking into account the risk likely to result from the processing for the rights and freedoms of [users]" (recital 98 GDPR). In the latter case, attention will also have to be paid in particular to the risks to the rights and freedoms of children which - as this Code shows - can be different to, or be fleshed out in a different way, than those of adults.

The goal of the code of practice is thus a correct application of the GDPR (also Article 40). In the code of practice, industry organisations can explain the application of the rules of the GDPR to the relevant industry (Article 40(2) GDPR). One of the subjects which a code of practice can encompass is "the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained" (Art. 40 (2) (g) GDPR). A code of practice can relate to a specific industry, like the British Age Appropriate Design Code for digital services, but can also focus on a specific design, like age verification.

The code of practice can receive the approval of the Dutch Data Protection Authority if it offers adequate safeguards (Article 40(5) GDPR). Industries with a "high risk", such as those where data of children are processed, are required to apply more stringent safeguards, in view of, e.g., the sensitivity of the personal data, the vulnerability of the data subject, or the invasive character of the data processing. Supervision of the compliance with a code of practice is carried out by an agency that possesses the appropriate expertise with regard to the subject-matter of the code of practice and was accredited to do so by the competent supervisory authority, in the Netherlands the Data Protection Authority (*Autoriteit Persoonsgegevens*) (Article 41 GDPR).

Consumer law

A code of practice is not without commitment and, as a business, you will have to comply with it. Failure to perform an obligation in a code of practice can be a misleading commercial practice (Article 6:193c(2) under a DCC).

Sources

Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)*, p. 28.

Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (PIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248*, 2017, p. 10, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Article 29 Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of the regulation 2016/679.* WP 251, 3 October 2017, p. 29.

Autoriteit Consument & Markt, *Leidraad Bescherming van de online consument: Grenzen aan online beïnvloeding*, 2020, https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf

Boom, W.H. van, *Inpassing en handhaving van de Wet oneerlijke handelspraktijken*, Tijdschrift voor Consumentenrecht en handelspraktijken, 2008.

College van Beroep voor het bedrijfsleven 15 May 2018, ECLI:NL:CBB:2018:145.

Consumer Protection Cooperation Network, *Common position of national authorities within the CPC [related to online games],* European Commission: 2013, https://ec.europa.eu/info/sites/info/files/common-position_of_national_authorities_within_cpc_2013_en_0.pdf.

Council of Europe, *Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Convention 108 (Guidelines), 2020, https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b.

Data Protection Commission, *Fundamentals for a Child-Oriented Approach to Data Protection* (Draft version for Public Consultation), Dublin: 2020, https://www.dataprotection.ie/en/dpc-guidance/blogs/the-children-fundamentals.

Dempsey, J., Sim, G. & Cassidy, B., *Designing for GDPR - Investigating Children's Understanding of Privacy: A Survey Approach*, 2018, http://clok.uclan.ac.uk/24179/1/BHCI-2018_paper_82.pdf

Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Recommendation CM/Rec(2018)7 of the Committee of Ministers), Council of Europe: 2018, https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-

rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html.

Hof, S. van der & Hannema, T.S.P., *Veilig opgroeien in een wereld vol algoritmes. De bijzondere bescherming van kinderen onder art. 22 Algemene Verordening Gegevensbescherming*, Privacy & Informatie 2018(6): 190-198.

Hof, S. van der & Lievens, E., *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): 2018, 33 -43. (DRAFT PAPER p. 7, p. 9)

Hof, S. van der, Lievens, E. & Milkaite, I., 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: Liefaard T., Rap S., Rodrigues P. (ed.) *Monitoring Children's Rights in the Netherlands. 30 Years of the UN Convention on the Rights of the Child.* Leiden: Leiden University Press, 2019, pp. 25, 35, 36, 38, 39. (DRAFT)

Information Commissioner's Office, *Age appropriate Design: a code of practice for online services,* 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.

Information Commissioner's Office, 'Right to Erasure": recital 65 GDRP. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/how-does-the-right-to-erasure-apply-to-children/

Information Commissioner's Office, *Consultation*: *Children and the GDPR guidance*, 2017, https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf.

International Telecommunication Union, *Guidelines for industry on Child Online Protection,* Geneva: 2020, https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_967b2ded811f48c6b57c7c5f68e58a02.pdf.

Kardefelt-Winther, D., Day, E., Berman, G., Winning, S.K., Bose, A., *Encryption, Privacy and Children's Right to Protection from Harm,* UNICEF Office of Research - Innocenti (Working Paper), 2020, https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html.

Kennisnet, *Waarde wegen: Een ethisch perspectief op digitalisering in het onderwijs,* Zoetermeer: 2020, https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Ethiekkompas-Waardenwegen.pdf.

Kolucki, B. & Lemish, D., *Communication with Children: Principles and Practices to Nurture, Inspire, Excite, Educate and Heal,* New York: UNICEF 2011, https://sites.unicef.org/cwc/files/CwC_Final_Nov-2011.pdf.

Pijpers, R. & Bosch, N. van den (ed.), *Positive Digital Content for Kids: Experts reveal their secrets.* POSCON & Mijn Kind Online, 2014, https://www.kennisnet.nl/mijnkindonline/files/Positive_digital_content_for_kids.pdf.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) no. 2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices Directive") (*Official Journal* 2005, L 149/22).

Roosendaal, A. & Privacy Company (2016), *Privacy by Design in de praktijk!* (Annual conference ECP), https://docplayer.nl/44346190-Privacy-by-design-in-de-praktijk.html.

UC Berkeley School of Information, "Privacy patterns", https://privacypatterns.org/.

Verdoodt, V. (2018), *Children's rights and advertising literacy in the digital era: towards an empowering regulatory framework for commercial communication.*

UNICEF, Child Rights and Online Gaming, Opportunities and challenges for children and the industry, Discussion paper, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

UNICEF, *Training Module 2: Child Online Protection Guidelines for ICT Industry,* Powerpoint presentation (n.d.), https://sites.unicef.org/csr/files/Training_Module_2_Child_Online_Protection_for_ICT_industry.pdf.

Statute of 25 September 2008 to amend Books 3 and 6 of the Dutch Civil Code and other statutes to comply with the Unfair Commercial Practices Directive, *Stb.* 2008, 397.

Additional reading material

Amnesty International rapport 'Surveillance Giants' (background): https://www.amnesty-international.be/nieuws/alomtegenwoordige-surveillance-van-facebook-en-google-is-gevaar-voor-mensenrechten

Autoriteit Consument & Markt leidraad 'Bescherming van de online consument': https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf

Data & Design by LINC (focus on GDPR): https://design.cnil.fr/en/

Defenddigitalme (focus on education): https://defenddigitalme.org/

Kinderrechten.nl: https://www.kinderrechten.nl/

OECD Council rapport 'The protection of children online' (recommendations for policy): https://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en

Tada: https://tada.city/en/home-en/

UNICEF (reports, articles and workshops relating to *AI for children*): https://www.unicef.org/globalinsight/featured-projects/ai-children

UNICEF (training modules): https://sites.unicef.org/csr/resources.html

Colophon

Simone van der Hof
Quirine van Eeden
Hannah Grijns
Rosalie Kok
Melis Bilgin
Hannah Volman
Tessel van Leeuwen
Sander van der Waal
Laurens Hebly

Our special thanks goes to Frank van der Meyden (Ministry of the Interior and Kingdom Relations).

The Code has been drawn up in consultation with experts in the intersection of child and technology, and with designers, developers and young people. We would hereby like to thank all participants in the expert sessions and all who read through the Code for their valuable input. In particular we would like to express our thanks to Robert Zuiverloon and his class, Alain Otjens, Anne-Jel Hoelen, Arnold Roosendaal, Astrid Poot, Douwe-Sjoerd Boschman, Eva Lievens, Fiona Vening, Lodewijk Loos, Marit Hoefsloot, Marjolijn Bonthuis, Simone Fennell-van Esch and Tom Demeyer. Any errors and inaccuracies are the responsibility of the drafters of the Code.

Annex. Communication with children per age category

Classification into age categories and recommendations come from the British Age Appropriate Design Code.

Communication with children per age category

Age category	Recommendations
0-5 *Pre-literate and early literacy -*	• use simple language, repetition, explain on the basis of rhythm and song with animals and people, use rhymes and riddles.
6-9 *Core primary school years*	• use stories about friendship, the creation of skills, daily incidents about someone's values and critical thinking capacity.
10-12 *Transition years*	• use of role models, tell stories about the influence of family, friends and media on the child, encourage children in their need to experiment at this age and dare to make independent choices.
13 - 15 *Early teens*	• use of role models, tell stories about the influence of family, friends and media on the child, encourage children in their need to experiment at this age and dare to make independent choices.

16-17 *Approaching adulthood*	• use of role models, tell stories about the influence of family, friends and media on the young, encourage children in their need to experiment at this age and dare to make independent choices.

Communication with children *about privacy* per age category

Age category	Recommendations
0-5 *Pre-literate and early literacy -*	• Provide complete privacy information as mandated in accordance with Articles 13 and 14 of the GDPR, in a form appropriate for parents. • Provide audio or video prompts which call on children to leave things as they are or to seek the assistance of a parent or trusted adult if they try to change high privacy default settings.
6-9 *Core primary school years*	• Provide complete privacy information as mandated in accordance with Articles 13 and 14 of the GDPR, in a form appropriate for parents. • In addition to the information for parents, provide cartoons or video or audio materials. • Provide explanation on the basic principles of online privacy within your service, the privacy settings which you provide, who can see what, their information rights, how they can control their own information and about respecting the privacy of others. • Explain the basic elements of your service and how it works, what they can expect of you and what you expect from them.

10-12 *Transition years*	• Provide complete privacy information as mandated in accordance with Articles 13 and 14 of the GDPR, in a form appropriate for parents. • Provide complete privacy information as mandated in accordance with Articles 13 and 14 of the GDPR, in a form appropriate for children in this age group. • Offer children the choice between written and video/audio options. • Offer children the option of upscaling or downscaling the information shown according to individual need (based on materials developed for an older or younger age group). • If a child tries to change a high privacy default setting, provide cartoons or written, video or audio materials to explain what will happen with his or her information and what risks are involved. • Tell children that they have to leave things the way they are or have to seek the assistance of a parent or a trusted adult before they change the setting.

13 - 15
Early teens

- Provide complete privacy information as mandated in accordance with Articles 13 and 14 of the GDPR, in a form appropriate for this age group.
- Offer the choice between written and video/audio options.
- Offer children the option of upscaling or downscaling the information shown according to individual need (based on materials developed for an older or younger age group).
- If a child tries to change a high privacy default setting, provide cartoons or written, video or audio materials to explain what will happen with his or her information and what risks are involved.
- Encourage children to ask an adult or a trusted adult for assistance and not to change the setting if they have doubts or do not understand what you have told them.
- In addition to the information geared to the child, present complete information in a manner appropriate for the parents.

16-17
Approaching adulthood

- Provide complete information in a form appropriate for this age group.
- Offer the choice between written and video/audio options.
- Offer children the option of scaling the information shown up or down according to individual need (based on materials developed for an older or younger age group).
- If a child tries to change a high privacy default setting, provide written, video or audio materials to explain what will happen with his or her information and what risks are involved.
- Encourage children to ask an adult or another trusted information source for advice and not to change the setting if they have doubts or do not understand what you have told them.
- In addition to the information geared to the child, present complete information in a manner appropriate for the parents.

code voor
kinderrechten